NUMBERS

L.F.Taylor

# NUMBERS

## L.F.Taylor

FABER

# Numbers

L. F. TAYLOR

'Curiosity is one of the few virtues common to all scientists but unfortunately today its satisfaction is mostly dependent upon expensive equipment and closely knit team work, says Mr. Taylor in his preface. 'The research laboratory of a Theory of Numbers enthusiast can, at a pinch, be equipped with nothing more than pencil and paper. And to anyone who hesitates to set up such a laboratory and embark upon his own research because of the view that it has all been done before and there is nothing left to discover I would say with emphasis that this is not true. In mathematics there is always another field beyond the hedge if one can only find the gap to crawl through.'

In *Numbers* Mr. Taylor suggests some ways in which the gaps may be found and encourages his readers to discover what lies beyond them, and the result is a book which everyone who is drawn to numbers and the problems that arise from them will find fascinating.

40*s*
£2.00
*net*

# NUMBERS

# NUMBERS

L. F. TAYLOR

London
FABER AND FABER

*First Published in 1970*
*by Faber and Faber Limited*
*24 Russell Square London WC1*
*Printed in Great Britain at*
*The Pitman Press, Bath*
*All rights reserved*

*ISBN 0 571 09322 1*

## CONTENTS

# PREFACE

I don't know whether many people ever bother to read prefaces but I feel that anyone who wishes to find what a book is about should at least be offered the opportunity at as early a stage as possible.

First I must make it clear that, although I hope there is something to be learned from this one, it is in no sense a 'teaching' book: its intended purpose is to interest potential mathematicians and to introduce them to a branch of arithmetic which may transform their schoolday impressions of the subject.

Curiosity is one of the few virtues common to all scientists but unfortunately today its satisfaction is mostly dependent upon expensive equipment and closely knit team work. The research laboratory of a Theory of Numbers enthusiast can, at a pinch, be equipped with nothing more than pencil and paper. And to anyone who hesitates to set up such a laboratory and embark upon his own research because of the view that it has all been done before and there is nothing left to discover I would say with emphasis that this is not true. In mathematics there is always another field beyond the hedge if one can only find the gap to crawl through.

The main themes of this book are 'Factorisation' and 'Prime Numbers' but there are some diversions into such topics as recurring decimals, additive series, a brief note on Diophantine equations and a few others. They have all been chosen because they are among those branches of Number Theory which I have found intensely interesting—and I hope some of this enthusiasm will rub off during the reading—and also because they show how unexpectedly some divergent lines of enquiry latch in together.

I have included a chapter (Finite Arithmetic) on elementary congruence technique since some knowledge of this brilliant invention is essential to any serious study of large numbers. For the same reason there is a brief note on the 'Converse of Fermat's Theorem' and its relation to composite numbers.

A number of tables of values and functions have been included in the text and the Appendix; these have the double service of providing examples for the former and at the same time saving the potential research worker a certain amount of muscular mathematics.

Most readers will, I am sure, find something about the properties of numbers which is new to them in the following pages. (How many professionals, for instance, know of a direct linkage between 1/79—having a recurring period of thirteen digits—and $\sqrt{2}$ which is irrational?)

However it is the amateur mathematician I have had most in mind in compiling the following notes, and in defining my conception of the term 'amateur' I cannot do better than quote J. E. Littlewood (*A Mathematician's Miscellany*, Methuen & Co. Ltd.).

'I constantly meet people who are doubtful, generally without due reason, about their potential capacity . . . If your education just included, or just stopped short of including, 'a little calculus', you are fairly high in the amateur class.'

Coming from such a master this is pretty heartening and I hope his words will encourage those who find enjoyment and relaxation in solving puzzles to apply their ingenuity to experimenting with numbers.

Finally I would like to stress that in studies of this nature it is particularly important that the reader takes more than a passive interest in the text and I have therefore ended each chapter with a few relevant exercises. (The answers will be found at the end of the book.)

I am greatly indebted to Mr. Nicholas E. Scripture for some valuable advice and a critical scrutiny of the manuscript.

# I COUNTING

(1) In this book we shall be concerned almost entirely with the integers. Those all too familiar numbers 1, 2, 3, . . . which go on interminably, each one formed by adding 'one' to the last.

When man first began to feel the need for more specific terms than his current equivalent sounds for 'a', 'few' and 'many' he began to count. And counting is the basis of all arithmetic for it involves the process of addition.

One can only speculate on the evolutionary processes that led up to the system of counting by the addition of units as we know it, or on the many experiments which must have been tried before we settled down to counting generally in bundles of ten units. It has been plausibly put forward that the decimal scale originated in our having ten fingers on which to count but the weights and measures and the monetary systems of the world give this view little support.

Be that as it may we now have a stable and familiar arithmetic which uses the ten symbols, 0, 1, 2, . . . 9, and expresses numbers greater than nine in a form of shorthand based on the powers of ten. Thus the number 'two thousand five hundred and seventy nine' contains $9 \times 10^0 + 7 \times 10^1 + 5 \times 10^2 + 2 \times 10^3$ units and is conventionally written 2579.

(In the power index notation $n^0 = 1$, and $n^1 = n$.) If 2579 is successively divided by ten the remainders 9, then 7, 5, and 2 are left, these being its own digits reading from right to left.

All very elementary of course, but only because we are so accustomed to this system that there is no longer any need to stop and think how the numbers we use are constructed. Their expreſsion as multiples of powers of ten is, as we shall see, well chosen but it is none the less a matter of pure convention and it should not be forgotten that the same numbers could just as well be expressed as multiples of powers of any base we care to choose.

In order to convert a number in the decimal scale to that of any other base it is only necessary to divide successively by the number of the new base writing down the remainders in the reverse order to that in which they appear. Converting the number 2579 into the scale of seven for instance we have:

| | Remainder |
|---|---|
| 7)2579 | 3 |
| 7) 368 | 4 |
| 7) 52 | 3 |
| 7) 7 | 0 |
| 1 | 1 |

the new expression now being written 10343, indicating that it is equal to:

$$\begin{array}{rcrcr} 3\times 7^0 = 3\times & 1 & = & 3 \\ 4\times 7^1 = 4\times & 7 & = & 28 \\ 3\times 7^2 = 3\times & 49 & = & 147 \\ 0\times 7^3 = & & & 0 \\ 1\times 7^4 = 1\times & 2401 & = & 2401 \\ & & & \overline{\underline{\underline{2579}}} \end{array}$$

It will be seen that in dividing by seven there can be no remainder greater than six and so the only digits that appear in this scale are 0, 1, 2, . . . 6. Similarly in the scale of two we require only the two digits 0 and 1.

For example:

| | |
|---|---|
| 2)2579 | 1 |
| 2)1289 | 1 |
| 2) 644 | 0 |
| 2) 322 | 0 |
| 2) 161 | 1 |
| 2) 80 | 0 |
| 2) 40 | 0 |
| 2) 20 | 0 |
| 2) 10 | 0 |
| 2) 5 | 1 |
| 2) 2 | 0 |
| 1 | 1 |

the decimal number 2579 now appearing as 101000010011 which states explicitly that it is equal to

$$2^0 + 2^1 + 2^4 + 2^9 + 2^{11}$$

In just the same way the number could be given in powers of any number greater than ten, say for example twenty-three. (The divisions by 23 are given here in condensed form.)

| | |
|---|---|
| 23)2579 | 3 |
| 23) 112 | 20 |
| 4 | 4 |

In writing this down we have to remember that the '20' must be regarded here as a single digit; this can be made clear by enclosing it in brackets and the new number now appears as 4(20)3 indicating that 2579 is also equal to $3 + (20 \times 23) + (4 \times 23^2)$.

It will be convenient to denote any arrangement of digits as $N_s$, in which $s$ represents the scale of notation employed: the observations that have been made can then be written concisely as follows,

$$\begin{aligned} (N_{10})\,2579 &= (N_7)\,10343 \\ &= (N_2)\,101000010011 \\ &= (N_{23})\,4(20)3 \end{aligned}$$

It is now seen that whilst the choice is quite arbitrary the 'powers of ten' notation presents a good all-round middle course for expressing numbers requiring more than one digit; the use of fewer symbols calls for longer strings of digits to represent a given number while more symbols would have meant more and longer multiplication tables to memorise.

(2) There are occasions, however, when scales other than the decimal can be used with advantage. One of these will have become familiar to readers through the widespread development of electronic digital computers. Here the binary system which employs the two digits 0 and 1, is readily correlated with the two (on-off) positions of an electrical switch whilst an increase in the number of digits is of small consequence.

Again, because the binary system's largest digit is 1, it follows that any number whatever can be expressed as the sum of single powers of 2. Thus it is a simple matter to multiply together any two numbers without going outside the ×2 multiplication table.

This is done quite easily by successively multiplying one of the numbers and dividing the other by two and then deleting those numbers in the increasing column which correspond with the even numbers in the other.

In effect we are thus finding by successive division those powers of two which are needed to represent one number, multiplying the other by $2, 2^2, 2^3,$ etc., and then rejecting the products which are not required.

For example: To find $37 \times 127 (= 4699)$.

| Divide by 2 | | Multiply by 2 |
|---|---|---|
| 37 | 1 | 127 |
| 18 | 0 | ~~254~~ |
| 9 | 1 | 508 |
| 4 | 0 | ~~1016~~ |
| 2 | 0 | ~~2032~~ |
| 1 | 1 | 4064 |
| | | 4699 = Answer. |

The left hand column will be familiar; in it we have converted $(N_{10})$ 37 to $(N_2)$ 100101 showing that

$$37 = 2^0 + 2^2 + 2^5 = 1 + 4 + 32.$$

The right hand column is made up of 127 multiplied in turn by $2^0, 2^1, 2^2, \ldots 2^5$, and from it we have deleted the products of $2, 2^3,$ and $2^4$, the remaining figures then being added. In practice there is no need to write down the first column remainders since the zeros occur alongside even numbers and these can consequently be used to locate the deletion lines.

The process is much simpler to carry out than to describe and it is rather surprising that it is not taught as a rule of thumb method in those schools whose children have difficulty with their multiplication tables.

(3) Apart from these instances one might readily conclude that there is little to be gained by any further study of scale-changing and indeed this is about as far as most textbooks take the subject. Nevertheless it is never safe to assume that any branch of mathematics has arrived at a dead-end and it will be seen that further developments are not only possible but of practical interest. But first it will be necessary to make a digression over well trodden ground.

There are two well known and simple tests for determining whether a given number is divisible by nine or eleven. For the former the digits of the number are added together to form another number and if this contains more than one digit the process is continued until only one remains. If this digit is 9 then the original number is exactly divisible by 9; any other resultant digit will be the remainder found on dividing the original number by 9. Thus the number 23456723 when divided by nine will leave the remainder 5, since $2 + 3 + 4 + 5 + 6 + 7 + 2 + 3 = 32$, and $3 + 2 = 5$. The rule, commonly known as 'casting out the nines', can also be applied to division by three, the remainder in the above case then being $5 - 3 = 2$.

Somewhat similarly a number is exactly divisible by eleven if the difference between the sums of its alternate digits is 0 or a multiple of eleven. For example 73645 is divisible by eleven since $(5 + 6 + 7) - (4 + 3) = 11$.

Now the numbers nine and eleven are respectively $10 - 1$, and $10 + 1$ and it would be reasonable to expect that the same rules apply to the divisors $s - 1$ and $s + 1$ when dealing with numbers expressed in the scale of $s$. Suppose for example we take the number $4571 (= 7 \times 653)$ and transpose it into the scale of 8, thus:

| | | |
|---|---|---|
| 8 | 4571 | 3 |
| | 571 | 3 |
| | 71 | 7 |
| | 8 | 0 |
| | 1 | 1 |

Thus $(N_{10})$ 4571 = $(N_8)$ 10733.
And since in the scale of 8 the 'nines' rule applies to division by 7 we have $3 + 3 + 7 + 1 = 14 = 2 \times 7$, and therefore 7 is a divisor of 4571.

(We could have continued, $14 = (N_8)$ 16. And $6 + 1 = 7$)

Or again, converting to the scale of six and using the 'eleven' rule we have:

$$(N_{10})\ 4571 = (N_6)\ 33055$$

and as $5 + 0 + 3 = 5 + 3$ it is shown that 4571 is divisible by $(6 + 1) = 7$.

The principle is in fact quite general and can be proved without difficulty. To take, for simplicity's sake, a specific example, in the decimal scale every number can be expressed as follows:

$a + 10b + 100c + 1000d + \ldots = a + b + 9b + c + 99c + d + 999d + \ldots = a + b + c + d + \ldots + 9m$ (a multiple of 9)

That is, the sum of the digits $a, b, c,$ etc. will be the remainder after dividing by nine.

The 'eleven' rule and a generalisation into any scale of notation can be deduced in an exactly similar manner.

(4) We can now begin to glimpse another practical use for the process of scale changing. In many mathematical operations it is often desirable to know whether a given number is prime, or if not what are its factors. Provided the number is not too large the straightforward approach is to make tentative divisions by the successive primes 7, 11, 13, 17, etc., until a factor is found or the square root of the number is reached. (Obviously if there is no factor less than the square root there cannot be one which is greater and the number must be prime.) From what we have seen above it will be clear that when working through the primes in this way there will occur many cases when two tests can be carried out by making a single scale change. Thus whenever two primes differ by two, that is when they are of the form $n - 1$ and $n + 1$ they can be tested simultaneously by changing the given number into the scale of $n$ and applying the 'nine' and 'eleven' rules to the new digits.

Let us suppose for example that in attempting to factorise the number 18383 all the primes up to and including 23 have been tested without a factor appearing. Now instead of continuing with trial divisions first by 29 and then by 31 we convert the number into the scale of 30, thus:

$$\begin{array}{r|r|r} 30 & 18383 & 23 \\ & 612 & 12 \\ & 20 & 20 \end{array}$$

Applying the two tests to the 'digits' of the new scale we have,

(*a*) $23 + 12 + 20 = 55$

(*b*) $23 + 20 - 12 = 31$

Since 55 is not a multiple of 29 then this is not a factor but the 'eleven' rule shows that 31 is. Dividing out we find that $18383 = 31 \times 593$ and as $31^2$ is greater than 593 the latter is also prime.

(5) Now whilst it is possible to test both the prime divisors 41 and 43 in one operation, the conversion into the scale of 42 is 'awkward' and it is doubtful whether much time would be saved. The method is clearly most effective when, as in the last example the divisors to be tested lie on either side of a multiple of ten (i.e. $10n \pm 1$).

But, just as 'casting out the nines' can be used to detect multiples of three—a factor of nine—the above method is equally applicable to primes which are factors of numbers of the forms $10n - 1$ and $10n + 1$. For instance the scale of fifty provides an immediate test for the divisors 7 and 17 because $49 = 7^2$, and $51 = 17 \times 3$.

Taking for example the number 12733 (which equals $7 \times 17 \times 107$) and converting to the scale of fifty, we have:

$$\begin{array}{rr|r} 50 & 12733 & 33 \\ & 254 & 4 \\ & 5 & 5 \end{array}$$

and we see that

$$33 + 4 + 5 = 42 = \text{a multiple of } 7$$
$$33 + 5 - 4 = 34 = \text{a multiple of } 17$$

This property leads at once to an extremely simple test for prime, or prime factors of, numbers of the form $10^n \pm 1$. In these cases no actual division is required to make the scale change as, for example $1317459 = (N_{1000})$, 1(317)(459). Now 999 is a multiple of 37, and $1001 = 7 \times 11 \times 13$ and

since $459 + 317 + 1 = 777 = \underline{37} \times 21$

and $459 + 1 - 317 = 143 = \underline{11} \times \underline{13}$

it is seen at once that 1317459 is exactly divisible by 11, 13 and 37, but not by 7.

In general a given number can be tested for divisibility by any of the factors of $10^n \pm 1$ by separating it into sets of $n$ digits from the right and then applying the 'nine' and 'eleven' rules to these sets.

Incidentally it will now be seen that the basic test for, say, divisibility by eleven is by no means the only one. In fact, since the successive numbers $10 + 1$, $100 - 1$, $1000 + 1$, $10000 - 1$, and so on are all multiples of eleven it is a simple matter to devise a test tailored to suit the magnitude of any given number. Briefly, the number is divided into large 'sets' and then, according to the number of digits per set the 'nine' or 'eleven' rules are applied until only a two digit number remains. If this is divisible by 11 then so is the original number.

Thus if we wish to find the remainder when the number 7970684847 is divided by 11 we proceed first with subtraction because the number can be separated into sets of five digits:

$$\begin{array}{r} 84847 \\ 79706 \\ \hline 5141 \end{array}$$

and then by addition of pairs of digits:

$$\begin{array}{l} 51 \\ 41 \\ \hline 92 = (11 \times 8) + 4. \end{array}$$

And therefore the remainder is 4.

(6) It will be convenient to draw up a table of 'easy' scale-changes showing the prime numbers to which the $(s - 1)$ and $(s + 1)$ rules can be applied as tests of divisibility. By 'easy' I mean those scales which do not in effect require successive division by any number greater than eleven.

After what has been said the following Table 1 should be self explanatory; the numbers in brackets are all primes whose divisibility can be tested by changing the given number into the scale '$s$', and it will be seen that all the primes less than 100 are covered with the exception of 73, 83, and 97. And with some of them a single scale-change may eliminate as many as four possible prime factors.

Provided we remember which column we are working in it is quite practicable to change horses in mid-stream. Suppose, for instance, it is required to find the remainder, if any, on dividing 123456 by 17, then we have,

$$\begin{array}{rr|lrr|l} 800 \mid & 123456 & 256 & & & \\ & 154 & 154 & & & \\ \cline{3-3} & & 410 & 50 \mid & 410 & 10 \\ & & & & 8 & 8 \\ \cline{6-6} & & & & & 2 = \text{remainder} \end{array}$$

The exceptions mentioned, namely 73, 83 and 97, could be dealt with in the scales of 220, 250 and 290 respectively but these do not present such simple divisors as the above.

**Table 1**

| Scale(s) | $s - 1$ | $s + 1$ |
|---|---|---|
| 10 | 9 (3) | (11) |
| 20 | (19) | 21 (7) |
| 30 | (29) | (31) |
| 40 | 39 (13) | (41) |
| 50 | 49 (7) | 51 (17) |
| 60 | (59) | (61) |
| 70 | 69 (23) | (71) |
| 80 | (79) | 81 |
| 90 | (89) | 91 (7, 13) |
| 100 | 99 (11) | (101) |
| 110 | (109) | 111 (37) |
| 200 | (199) | 201 (67) |
| 300 | 299 (13, 23) | 301 (7, 43) |
| 800 | 799 (17, 47) | 801 (89) |
| 900 | 899 (29, 31) | 901 (17, 53) |
| 1000 | 999 (37) | 1001 (7, 11, 13) |

### EXERCISES

1. Express the integer 11111 in the scale of 2.
2. Express the integer 11111 in the scale of 16.
3. Express the integer 11111 in the scale of 32.
4. What observations can you find to make on the answers to exercises 1, 2, 3, ?
5. Multiply 123 by 456 by the process shown in the text and check by reversing the procedure.
6. Without using ordinary long division find what remainder, if any, is left after dividing $N = 455331$ by 707.

# 2 CASTING OUT THE PRIMES

(1) In the last chapter we saw how it was possible to tell whether a given number was a multiple of certain primes by dividing it, in effect, by a smaller number. The method was developed by generalising two well-known arithmetical tricks. Let us look at these two again from another angle.

Numbers in the decimal scale which are exactly divisible by nine are recognisable at once, as shown in *1*, 3), from the fact that the sum of their digits is always nine or some multiple of nine, thus:

$$\begin{array}{lcl} 2 \times 9 = 18 & \text{and} & 8 + 1 = 9 \\ 3 \times 9 = 27 & \text{and} & 7 + 2 = 9 \\ 4 \times 9 = 36 & \text{and} & 6 + 3 = 9 \\ 29773 \times 9 = 267957 & \text{and} & 7 + 5 + 9 + 7 + 6 + 2 = 36 \end{array}$$

and so on.

The above test deals with the number $10t - 1$, where $t = 1$. It would be natural to expect that similar rules could be devised for those numbers where $t$ takes the values 2, 3, 4, . . ., and it is readily seen that this is indeed the case.

Taking, for instance, some multiples of 19, where $t = 2$, and operating upon them by first multiplying the 'units' digit by two and then adding the result to the 'tens' digit it is found that the new number is then either 19 or a smaller multiple of 19. In the latter case the operation is repeated as in the method of 'casting out the nines'.

$$\begin{array}{r} 38 \\ \underline{16} \\ 19 \end{array} \quad \begin{array}{r} 57 \\ \underline{14} \\ 19 \end{array} \quad \begin{array}{r} 76 \\ \underline{12} \\ 19 \end{array} \quad \begin{array}{r} 247 \\ \underline{14} \\ 38 \\ \underline{16} \\ 19 \end{array} \quad \begin{array}{r} 84493 \\ \underline{6} \\ 8455 \\ \underline{10} \\ 855 \\ \underline{10} \\ 95 \\ \underline{10} \\ 19 \end{array} \; (= 19 \times 4447)$$

Similarly when $t = 3$, and it is desired to test for multiples of 29, the multiplier now becomes 3 and we have:

$$\begin{array}{r} 58 \\ \underline{24} \\ 29 \end{array} \quad \begin{array}{r} 87 \\ \underline{21} \\ 29 \end{array} \quad \begin{array}{r} 3393 \\ \underline{9} \\ 348 \\ \underline{24} \\ 58 \\ \underline{24} \\ 29 \end{array} \quad \begin{array}{r} 12673 \\ \underline{9} \\ 1276 \\ \underline{18} \\ 145 \\ \underline{15} \\ 29 \end{array} \; (= 29 \times 437)$$

The principle is clearly general and can perhaps best be explained by re-examining the procedure when $t = 2$. What we did, in effect, was to multiply the units digit by 19, or $(20 - 1)$, add, and then divide by 10.

For example

$$\begin{array}{r} 38 \\ \underline{152} \\ 19 \end{array} \; = 8 \times 19$$

Now let us suppose that $N = 19m = a + 10b$. Then, adding $19a$, we have $19a + a + 10b = 10(2a + b)$. Since 10 is not a divisor of 19 then $2a + b$ must be another multiple of 19 less than $19m$ and if the process is continued we must eventually arrive at the smallest possible multiple, namely 19 itself.

Looking again at the examples given above it will be seen that when $N$ is exactly divisible by 19 the process discloses the quotient $m$. For instance, in the case of $N = 247$ we have:

$$\begin{array}{r} 24\underline{7} \\ \underline{14} \\ 3\underline{8} \\ \underline{16} \\ 19 \end{array} \quad \text{is 'shorthand' for} \quad \begin{array}{rl} 247 & = 19m \\ \underline{133} & = 19 \times 7 \\ 380 & \\ \underline{1520} & = 19 \times 80 \\ 1900 & = 19 \times 100 \end{array}$$

Therefore $\quad 19m + (19 \times 7) + (19 \times 80) = 19 \times 100$

or
$$m = 100 - 87 = 13$$

In the algorithm the underlined digits, 87, provide us with $m$ after subtraction from 100.

Similarly when $N = 84493$ the terminal digits show that since

$$10000 - 5553 = 4447, \text{ then } 84493 = 19 \times 4447.$$

Or again, where we were dealing with multiples of 29, in the case of $N = 12673$, the terminal digits are 563.

Then $1000 - 563 = 437$ and hence $12673 = 29 \times 437$.

(2) It is important at this stage to note that nothing has been said to imply that this method of division only has its uses when $10t - 1$ is a prime. In fact it can be applied with the same advantage to any of the prime factors of $10t - 1$, as the following examples will show.

Since $13 \times 3 = 39$, we can use 4 as the multiplier to show that 4771 is a multiple of 13 thus:

$$\begin{array}{r} 4771 \\ \underline{4} \\ 481 \\ \underline{4} \\ 52 \\ \underline{8} \\ 13 \end{array}$$

And, multiplying the terminal digits 211 by 3 and subtracting from 1000 we have the quotient 367.

Similarly, noting that $13 \times 23 = 299$, it will be clear that, using the multiplier 30 as above, it is possible to test both these factors simultaneously.

Given $N = 12029\ (= 23 \times 523)$ then,

$$\begin{array}{r} 12029 \\ \underline{270} \\ 1472 \\ \underline{60} \\ 207 \\ \underline{210\phantom{0}} \\ 23\phantom{0} \end{array}$$

Thus 23 is a factor of 12029 but 13 is not. The quotient can be found as in the previous example.

(3) It is more than likely that the reader is already anticipating the next step in developing these principles. If this is so it might be a good thing for him to close the book at this point—temporarily I hope—and conduct some experiments of his own.

Whether this suggestion is acted upon or not our experience of the effects of scale-changing make it imperative to examine the treatment of those divisors which have, or can be put into, the form of $10t + 1$. As one might expect the method of test depends again upon the value of $t$, and it is quickly seen that by multiplying by $t$, etc., as in *2*.1, but in this case *subtracting*, any multiple of $10t + 1$ finally yields the digit 0.

Thus when $t = 2$ we have:

$$\begin{array}{rrl} 42 & 105 & 30639\ (= 21 \times 1459) \\ \underline{4} & \underline{10} & \phantom{0}\underline{18} \\ 0 & 0 & 3045 \\ & & \phantom{0}\underline{10} \\ & & 294 \\ & & \phantom{00}\underline{8} \\ & & 21 \\ & & \phantom{0}\underline{2} \\ & & \phantom{0}0 \end{array}$$

What is more, as the last example shows, the terminal digits 1 4 5 9 indicate the quotient directly.

As before the test is equally applicable to the factors of $10t + 1$ when this number is composite. In such cases, however, the method may produce a small multiple of the prime under test instead of zero, and the quotient is then rather more elusive. In order to keep this chapter within reasonable bounds I shall give only one example of this particular condition and the reader will be left to discover a general process for finding the quotient.

Let $N = 321433\ (= 47 \times 6839)$. Now $47 \times 3 = 141$, and we shall use the 'multiplier' 14, thus:

$$\begin{array}{r} 321433 \\ \underline{42} \\ 32101\phantom{0} \\ \underline{14}\phantom{0} \\ 3196\phantom{00} \\ \underline{84}\phantom{00} \\ 235\phantom{000} \\ \underline{70}\phantom{000} \\ -47\phantom{000} \end{array}$$

This example has been given not only to illustrate the above statement but also to show that in many cases this method of testing possible divisors of $N$ has a distinct advantage over the scale-changing technique. As we saw in Chap. 1 the latter is at its best when it can be applied to primes related to what I have called 'easy' divisors. On the other hand, in this system however large we have to make $t$ it has only to be multiplied by the terminal digits, none of which of course can be greater than 9.

(4) As we shall see later, when it comes to the factorisation of large numbers it is important to eliminate as many as possible of the small prime factors before starting on more sophisticated techniques. In the ordinary way this is a laborious process and any method of shortening the work is to be welcomed. The algorithm we have been experimenting with provides such a method and it will now be convenient to gather together our findings into a form available for easy reference.

To test whether a given number is exactly divisible by a prime $p$, choose a suitable multiple of $p$ such that

$$mp = 10t - 1 \quad \text{or} \quad 10t + 1$$

CASE A *Where* $mp = 10t - 1$.

The number to be tested ($N$) will, in the decimal scale be of the form $N = 10b + a$. From this derive the number $N_1 = b + ta$. $N_1$ then equals $10d + c$, and again from this derive $N_2 = d + tc$. Continue in this manner and if eventually a number $N_n$ is reached which equals either $p$ or a small multiple of $p$ then $p$ is an exact divisor of $N$.

CASE B *Where* $mp = 10t + 1$.

Again given that $N = 10b + a$, the numbers $N_1 = b - ta$, $N_2 = d - tc$, and so on are formed successively as above. If eventually it is found that $N_n = 0$, or $p$, or a small multiple of $p$, then $p$ is an exact divisor of $N$.

This sounds, and probably is, an unnecessarily formal way of describing a process which is extremely easy to operate in practice. This is a difficulty which is bound to arise when one employs methods which do not appear in ordinary arithmetic and is the principle reason why so many examples have been presented.

Now whilst $m$ can be chosen so that $pm$ is equal to either of the numbers $10t \pm 1$ it will be obvious that for the purpose we have in mind one of these will be preferable to the other. For instance, if we wish to test whether 23 is a divisor then we have $23 \times 3 = 69$, and $t = 7$. To find a multiple of 23 of the form $10t + 1$ we would have to take $23 \times 7 = 161$, $t$ then becoming 16. Neither of these values presents any difficulty but I think most people would choose 7 as the multiplier and the 'addition' process for the test.

In the following table the primes below one hundred are listed together with their appropriate testing multipliers $t(+)$ and $t(-)$.

**Table 2**

| $p$ | $t(+)$ | $t(-)$ | $p$ | $t(+)$ | $t(-)$ |
|---|---|---|---|---|---|
| 7 | 5 | 2 | 47 | 33 | 14 |
| 11 | 10 | 1 | 53 | 16 | 37 |
| 13 | 4 | 9 | 59 | 6 | 53 |
| 17 | 12 | 5 | 61 | 55 | 6 |
| 19 | 2 | 17 | 67 | 47 | 20 |
| 23 | 7 | 16 | 71 | 64 | 7 |
| 29 | 3 | 26 | 73 | 22 | 51 |
| 31 | 28 | 3 | 79 | 8 | 71 |
| 37 | 26 | 11 | 83 | 25 | 58 |
| 41 | 37 | 4 | 89 | 9 | 80 |
| 43 | 13 | 30 | 97 | 68 | 29 |

(5) The methods so far described have been developed from elementary properties of numbers and are in fact nothing more than extensions of the well-known rules for 'casting out the nines' and detecting multiples of eleven. Constructing algorithms of this sort is always an interesting—and often rewarding—form of mathematical recreation and it is surprisingly easy to devise divisibility tests from purely empirical observations.

For instance the fact that $17 \times 6 = 102$, immediately suggests a simple method of dividing by 17. One has only to double the left-hand digit, subtract from the next pair of digits and continue in this manner, thus:

$$N = 13579\,(= (17 \times 798) + 13)$$

$$\begin{array}{rl}
\underline{1}3579 & \\
2\phantom{79} & \\
\hline
379 & \\
6\phantom{9} & \\
\hline
\underline{3}19 & \\
6 & \\
\hline
13 & = \text{the remainder.}
\end{array}$$

Multiplying the underlined digits 133 by 6, (102/17) gives us 798 which is the quotient.

We could, of course, have paired the digits off from the right and proceeded:

$$\begin{array}{rrr}
1 & 35 & 79 \\
 & 2 & \\
\cline{2-2}
 & 33 & 79 \\
 & & 66 \\
\cline{3-3}
 & & 13
\end{array}$$

This system is merely long division in a slightly different dialect but it is clearly preferable when dealing with large numbers and divisors which are closely adjacent to powers of 10. Thus one of our earlier 'awkward' divisors, 97, presents no difficulty when it is treated as (100 − 3). Here we use the multiplier 3 and add, as in the example,

$$N = 1234567\,(= (97 \times 12727) + 48)$$

$$\begin{array}{rl}
\underline{1}234567 & \\
3\phantom{4567} & \\
\hline
\underline{2}64567 & \\
6\phantom{567} & \\
\hline
\underline{7}0567 & \\
21\phantom{67} & \\
\hline
\underline{2}667 & \\
6\phantom{7} & \\
\hline
\underline{7}27 & \\
21 & \\
\hline
48 & = \text{the remainder}
\end{array}$$

And again the underlined digits provide the quotient. Obviously it is a very simple matter to divide by any of the factors of numbers of the forms 9999 . . . 99, and 1000 . . . 01.

I have yet to meet a 'Theory of Numbers' addict who can resist a problem and to round off this chapter I present the following little curiosity. Again use is made of the '$t$' function, this time in the form of the rising powers $t^0, t^1, t^2, \ldots t^n$, (note that $t^0 = 1$, $t^1 = t$), and the two worked instances should make the principle plain without the need of verbal explanation.

(*A*) $N = 31711 = 19 \times 1669.$ $(t = 2)$

$$\begin{array}{rcrcr}
3 & \times & 1 & = & 3 \\
1 & \times & 2 & = & 2 \\
7 & \times & 4 & = & 28 \\
1 & \times & 8 & = & 8 \\
1 & \times & 16 & = & \underline{16} \\
 & & & & 57 \\
 & & & & \\
5 & \times & 1 & = & 5 \\
7 & \times & 2 & = & \underline{14} \\
 & & & & \underline{\underline{19}}
\end{array}$$

(*B*) $N = 34561 = 17 \times 2033.$ $(t = 5)$

$$\begin{array}{rcrcr}
3 & \times & 1 & = & 3 \\
4 & \times & 5 & = & 20 \\
5 & \times & 25 & = & 125 \\
6 & \times & 125 & = & 750 \\
1 & \times & 625 & = & 625
\end{array}$$

Now applying the 'eleven' rule we have,

$$(20 + 750) - (3 + 125 + 625) = 770 - 753 = 17.$$

The point of interest is that the increasing powers of $t$ are applied in the opposite direction (that is, from left to right) to what one might expect.

### EXERCISES

1. If $43n = 21010101$, find $n$ by two different calculations, but without using 'long division'.
2. What remainder is left after dividing 110999999 by 997?
3. Devise a simple process for dividing by 167.

# 3 RECURRING DECIMALS

(1) If we take a large multiple of ten, say $10^n$ where $n > 20$, and divide it in the normal manner by 19 we produce the sequence of digits 526315789473684210526 3 . . . which repeat themselves in bunches of eighteen digits. Dividing this number by the appropriate $10^n$ we are then able to say that $1/19 = \cdot\dot{0}5263157894736842\dot{1}$, the suffixed periods indicating that this decimal part is repeated over and over again.

There is a simple but important distinction to be observed here. The decimal ·9999 . . ., in which the 9's are continued indefinitely, and usually expressed as $\cdot\dot{9}$, is indistinguishable from unity and the above decimal $\cdot\dot{0}52 \ldots 842\dot{1}$ is an exact divisor of $\cdot\dot{9}$. On the other hand the number 526 . . . 421 is an exact divisor of 999,999,999,999,999,999. Similarly 142857 is a divisor of 999,999 and hence $\cdot\dot{1}4285\dot{7}$ is a divisor of $\cdot\dot{9}$: it is in fact equal to 1/7.

Reverting again to the fraction 1/19, we saw in the last chapter that division by 19 can be done, in effect, by multiplying successively by 2 starting from the right. It will be seen at once that, starting with the digit 1, the above decimal is an excellent example of this process.

Thus, following this procedure we have:

```
                     168421
                    32
                   64
                 128
                256
               512
             1024
            2048
           4096
          8192
        16384
       32768
      65536
    131072
   262144
  524288
1048576
etc.
     ______________________
     4210526315789473684210
```

which, continued indefinitely produces the decimal recurrent cycle of the fraction 1/19. Another way of expressing the above summation is $20^0 + 20^1 + 20^2 + 20^3 + \ldots$, which of course can be summed as follows,

```
          1
         20
        400
       8000
     160000
    3200000
       etc.
    _______
. . .368421
```

The above sequence of digits can be arrived at in a number of ways. Two of these will be illustrated next in order to indicate the diversity of approach which this subject provides.

The following tabulation will probably demonstrate one method more clearly than any laboured description of the process.

Three columns, $A$, $B$, and $C$ are set up in which $B_n$ is the integral part of $A_n/2$ and $C_n$ is the remainder. The $A_n$ entries, starting with 1, are found from the relationship

$$A_{n+1} = 10C_n + B_n$$

| A | B | C |
|---|---|---|
| 2 into 1 | = 0 remainder | 1 |
| 10 | 5 | 0 |
| 5 | 2 | 1 |
| 12 | 6 | 0 |
| 6 | 3 | 0 |
| 3 | 1 | 1 |
| 11 | 5 | 1 |
| 15 | 7 | 1 |
| 17 | 8 | 1 |
| 18 | 9 | 0 |
| 9 | 4 | 1 |
| 14 | 7 | 0 |
| 7 | 3 | 1 |
| 13 | 6 | 1 |
| 16 | 8 | 0 |
| 8 | 4 | 0 |
| 4 | 2 | 0 |
| 2 | 1 | 0 |
| 1 | 0 | 1 |

Column *B* then provides the required sequence of digits.

The next example is again best expressed in columnar form. This time the successive *A* entries are multiplied by 10 and we have the relationship $A_{n+1} = 10C_n - B$, where *B* is the largest multiple of 19 less than $A_{n+1}$.

| | A | | B | | C |
|---|---|---|---|---|---|
| 10 × | 1 | − | 0 | = | 10 |
| 10 × | 10 | − | 95 | = | 5 |
| 10 × | 5 | − | 38 | = | 12 |
| 10 × | 12 | − | 114 | = | 6 |
| 10 × | 6 | − | 57 | = | 3 |
| 10 × | 3 | − | 19 | = | 11 |
| 10 × | 11 | − | 95 | = | 15 |
| 10 × | 15 | − | 133 | = | 17 |

and so on.

The curiosity here is that the 'units' digits of column *C* are now those of column *B* in the last example whilst the 'tens' digits (which are to be ignored for the present purpose) occur in exactly the same positions as the remainders '1' appeared in the previous column *C*.

I am sure readers would find it entertaining to find for themselves the corresponding techniques for determining the recurring cycles of the fraction 1/29. There are, as one might expect, close relationships amongst all fractions of the form $1/(10n \pm 1)$ and it is not difficult, reasoning by analogy, to formulate general constructions.

(2) These periodic sequences of digits relating to the common fractions have many curious properties, not all of them as predictable as one might expect and in order to observe some of them and to provide enough material for further experiment it will be useful to have before us a sufficient number of examples. Table 3 lists the decimal equivalents of the reciprocals of the prime numbers from 7 to 97 inclusive.

### Table 3

**Recurrent Period of 1/*p*. (*p*—prime)**

| *p* | |
|---|---|
| 7 | ·142857 |
| 11 | ·09 |
| 13 | ·076923 |
| 17 | ·0588235294117647 |
| 19 | ·052631578947368421 |
| 23 | ·0434782608695652173913 |
| 29 | ·0344827586206896551724137931 |
| 31 | ·032258064516129 |
| 37 | ·027 |
| 41 | ·02439 |
| 43 | ·023255813953488372093 |
| 47 | ·0212765957446808510638297872340425531914893617 |
| 53 | ·0188679245283 |
| 59 | ·0169491525423728813559322033898305084745762711864406779661 |
| 61 | ·016393442622950819672131147540983606557377049180327868852459 |
| 67 | ·014925373134328358208955223880597 |
| 71 | ·01408450704225352112676056338028169 |
| 73 | ·01369863 |
| 79 | ·0126582278481 |
| 83 | ·01204819277108433734939759036144578313253 |
| 89 | ·01123595505617977528089887640449438202247191 |
| 97 | ·010309278350515463917525773195876288659793814432989690721649484536082474226804123711340206185567 |

It will be seen at once that roughly half of these periods contain $(p - 1)$ digits whilst the rest have some fraction of $(p - 1)$. When the denominator of the original common factor is composite (say *m*) the number of digits in the period is, however, invariably less than *m*. For further reference and to provide material for any reader who wishes to pursue the subject, Tables 4 and 5 give the decimal equivalents of the reciprocals of some composite numbers.

### Table 4

**Recurrent period of 1/*m*. (*m*—composite, $\neq 2k$, $5k$, or $k^2$)**

| *m* | |
|---|---|
| 21 | ·047619 |
| 27 | ·037 |
| 33 | ·03 |
| 39 | ·025641 |
| 51 | ·0196078431372549 |
| 57 | ·017543859649122807 |
| 63 | ·015873 |
| 69 | ·0144927536231884057971 |
| 77 | ·012987 |
| 87 | ·0114942528735632183908045977 |
| 91 | ·010989 |
| 93 | ·010752688172043 |

### Table 5

**Recurrent period of $1/p^2$. ($p \neq 2k$ or $5k$)**

| $p^2$ | |
|---|---|
| 49 | ·020408163265306122448979591836734693877551 |
| 81 | ·012345679 |
| 121 | ·0082644628099173553719 |
| 169 | ·005917159763313609467455621301775147928994082840236686390532544378698224852071 |
| 289 | ·0034602076124567474048442906574394463667820069204152249134948096885813148788927335640138408304498269896193771626297577854671280276816608996539792387543252595155709342560553633217993079584775086505190311418685121107266435986159169550173010380622837370242214532871972318339 1 |
| 361 | ·0027700831024930747922437673130193905817174515235457063711911357340720221606648199445983379501385041551246537396121883656509695290858725761772853185595567867036011080332409972299168975069252077562326869806094182825484764542936288088642659279778393351800554016620498614958448753462603878116343490304709141274238227146814404432132963988919667 59 |
| 441 | ·002267573696145124716553287981859410430839 |

(3) With these tables we now have enough material to make a number of observations of the properties and methods of construction of these interesting periodic sequences.

As we saw at the beginning of this chapter the fraction 1/19 is generated by multiplying successively by the '*t*' function (see Table 2) from the right and starting with unity. This method is quite generally applicable and is not restricted to prime denominators. For instance the decimal equivalent of 1/39 as seen in Table 3 is $0{\cdot}\dot{0}2564\dot{1}$, obtained by using the multiplier 4.

Thus:

```
                1
               4
             16
            64
          256
         1024
        4096       etc.
     -----------
     . . . 1025641
```

Multiplying this sequence by three gives . . . 3076923 . . . (1/13). Of course the periodic part of the fraction 1/13 could have been obtained directly by multiplying as before by four but starting with the digit 3, thus:

```
                3
              12
             48
           192
          768
         3042
       12288       etc.
     -----------
     . . . 3076923
```

Similarly, using ×5, and starting with 7 we obtain the sequence . . . 142857 for the fraction 1/7.

Using the above principles together with the '*t*' functions in Table 2, we have then a general method for producing the periodic parts of any fraction whose denominator is not a multiple of two or five.

There are many other ways of doing this. As an example of one employing a more orthodox arithmetic than the above we may note that on dividing seven into one hundred a remainder of two is left; the following two hundred then has a remainder of four, and so on. The decimal equivalent of 1/7 can then be quickly written down by multiplying the first dividend by two, placing the result two places to the right and continuing in this way, thus:

```
14
  28
    56
     112
       224
         448   and so on.
--------------
1428571428 . . .
```

This example was chosen because it is often quoted as a curiosity; in fact since $10 - 7 = 3$ it is just as effective to use 3/10 as the multiplier.

```
1
 3
  9
  27
   81
   243
    729
    2187
     6561
     19683
      59049
-------------
1428571 . . .
```

Being a straightforward substitute for long division there are no restrictions in this process and for example the fraction 1/8 can be calculated in an exactly similar manner. Here $8 = 10 - 2$ and we have,

```
      1
       2
        4
         8
         16
          32
           64
           128
            256 . . .
--------------
. . . 1249999 . . .   = ·125
```

The method is obviously quite general, its main charm as a computational time-saver arising when the denominator of the required fraction or one of its multiples is close to and a little less than a power of ten. For instance, noting that 17 × 588 = 9996 = 10000 − 4, we can rapidly decimalise 1/17 by multiplying ·0588 successively by 4/10000, thus:

$$\begin{array}{l}
0588\\
\phantom{00}2352\\
\phantom{0000}9408\\
\phantom{00000}37632\\
\phantom{000000}150528\\
\phantom{00000000}602112\ldots\\
\hline
05882352941176470588\ldots
\end{array}$$

The above examples lead back in a roundabout way to the second paragraph of this chapter, for clearly if a fraction's denominator is a factor of $10^n - 1$, then the multiplier is unity. In such cases it is easy now to see that since, say, 999 = 37 × 27, then 1/37 = ·0270270 . . . = $\cdot\dot{0}2\dot{7}$, and as 99999 = 41 × 2439, then 1/41 = $\cdot\dot{0}243\dot{9}$.

The situation changes in a curious and less obvious manner when a denominator, or one of its multiples, is treated as exceeding a power of ten. Taking again 1/17 as an example we have 17 × 6 = 102, and we now use the multiplier 2/100 but this time alternately add and subtract the successive multiples. Thus:

$$\begin{array}{rl}
+ & \cdot 06\\
- & \phantom{\cdot 00}12\\
\hline
 & \cdot 0588\\
+ & \phantom{\cdot 0000}24\\
\hline
 & \cdot 058824\\
- & \phantom{\cdot 000000}48\\
\hline
 & \cdot 05882352\\
+ & \phantom{\cdot 00000000}96\\
\hline
 & \cdot 0588235296\\
- & \phantom{\cdot 000000000}192\\
\hline
 & \cdot 058823529408\\
+ & \phantom{\cdot 00000000000}384\\
\hline
 & \cdot 05882352941184\\
- & \phantom{\cdot 0000000000000}768\\
\hline
 & \cdot 0588235294117632\\
+ & \phantom{\cdot 00000000000000}1536\\
\hline
 & \cdot 058823529411764736\\
- & \phantom{\cdot 0000000000000000}3072\\
\hline
 & \cdot 058823529411764705\ldots
\end{array}$$

By a similar process, and noting that 7 × 143 = 1001, we have a still quicker method for determining 1/7, namely,

$$\begin{array}{rl}
+ & \cdot 143\\
- & \phantom{\cdot 000}143\\
\hline
 & \cdot 142857\\
+ & \phantom{\cdot 000000}143\\
\hline
 & \cdot 14285714\ldots
\end{array}$$

(4) It is in fact amazing how many algorithms can be devised for constructing the recurring periods of decimal fractions. Added to what has already been shown the following three examples will indicate something of the richness of this field.

*Example* 1. 1/31

$$\begin{array}{lcr}
 & & 29\\
2\times 29+3 &=& 61\phantom{0}\\
2\times 61+29 &=& 151\phantom{00}\\
2\times 151+61 &=& 363\phantom{000}\\
2\times 363+151 &=& 877\phantom{0000}\\
2\times 877+363 &=& 2117\phantom{00000}\\
2\times 2117+877 &=& 5111\phantom{000000}\\
2\times 5111+2117 &=& 12339\phantom{0000000}\\
2\times 12339+5111 &=& 29789\phantom{00000000}\\
\cline{3-3}
 & & \ldots 29032258064516129
\end{array}$$

*Example* 2. 1/29

$$\begin{array}{lcr}
 & & 31\\
9\times 31 &=& 279\phantom{0}\\
9\times 279 &=& 2511\phantom{00}\\
9\times 2511 &=& 22599\phantom{000}\\
9\times 22599 &=& 203391\phantom{0000}\\
9\times 203391 &=& 1830519\phantom{00000}\\
\cline{3-3}
 & & \ldots 551724137931
\end{array}$$

*Example* 3. 1/67

$$\begin{array}{lcl}
 & & \cdot 01\\
 & & \phantom{\cdot 01}49\\
(1+49)/2 &=& \phantom{\cdot 0149}25\\
(49+25)/2 &=& \phantom{\cdot 014925}37\\
(25+37)/2 &=& \phantom{\cdot 01492537}31\\
(37+31)/2 &=& \phantom{\cdot 0149253731}34\ldots\\
\cline{3-3}
 & & \cdot 014925373134\ldots
\end{array}$$

(5) There are some still more remarkable ways in which these periodic sequences can be formed, illustrating in a striking manner how an unsuspected common link can sometimes be found between apparently unrelated branches of Number Theory. It will be more convenient, however, to examine these after introducing in the next chapter the curious additive series associated with the name of Fibonacci.

From the constructions already given it will have become clear that fractions which have recurrent, or cyclic, periods can also be expressed by the summation of infinite series. We have seen, in effect, that 1/7 ($= 0{\cdot}\dot{1}4285\dot{7}$) is equivalent to

$$\frac{1}{10}+\frac{3}{10^2}+\frac{3^2}{10^3}+\frac{3^3}{10^4}+\ldots$$

and also to

$$\frac{14}{10^2}+\frac{28}{10^4}+\frac{56}{10^6}+\frac{112}{10^8}\ldots$$

which is the same as

$$\frac{7}{50}+\frac{7}{50^2}+\frac{7}{50^3}+\ldots$$

and again, to

$$\frac{143}{10^3}-\frac{143}{10^6}+\frac{143}{10^9}-\ldots$$

It might also be noted that the series for 1/19 and 1/21 can be simplified into the following forms:

$$1/19 = 1/20 + 1/20^2 + 1/20^3 + \ldots$$
$$1/21 = 1/20 - 1/20^2 + 1/20^3 - \ldots$$

In general, if we express $N$ as one of the forms $(10^n \pm a)/s$ the series for $1/N$ then becomes:

$$(1)\qquad \frac{1}{N}=\frac{s}{10^n-a}=\frac{sa}{10^n}+\frac{sa^2}{10^{2n}}+\frac{sa^3}{10^{3n}}+\ldots$$

$$(2)\qquad \frac{1}{N}=\frac{s}{10^n+a}=\frac{sa}{10^n}-\frac{sa^2}{10^{2n}}+\frac{sa^3}{10^{3n}}-\ldots$$

Some of the cyclic properties of recurrent decimals are of common knowledge, particularly the confined cycle which occurs when $1/N$ has a period consisting of $N-1$ digits. With a denominator of seven, for instance, the corresponding six fractions are:

$$\begin{aligned}
1/7 &= 0{\cdot}142857\ldots\\
2/7 &= 0{\cdot}285714\ldots\\
3/7 &= 0{\cdot}428571\ldots\\
4/7 &= 0{\cdot}571428\ldots\\
5/7 &= 0{\cdot}714285\ldots\\
6/7 &= 0{\cdot}857142\ldots
\end{aligned}$$

This recycling of the same digits in the same order is to be found in the fractions 1/17, 1/19, 1/23, 1/29, 1/47, 1/59, 1/61, 1/67, 1/97, . . ., but it obviously cannot occur when the number of digits in the cycle is less than $N - 1$. Thus when $N$ is 13 and 1/13 has the decimal equivalent of ·076923 employing only $(N - 1)/2$ digits, we have two sets of recycling digits.

$$\begin{array}{rlrl}
1/13 = & \cdot 076923\ldots, & 2/13 = & \cdot 153846\ldots \\
3/13 = & \cdot 230769\ldots, & 5/13 = & \cdot 384615\ldots \\
4/13 = & \cdot 307692\ldots, & 6/13 = & \cdot 461538\ldots \\
9/13 = & \cdot 692307\ldots, & 7/13 = & \cdot 538461\ldots \\
10/13 = & \cdot 769230\ldots, & 8/13 = & \cdot 615384\ldots \\
12/13 = & \cdot 923076\ldots, & 11/13 = & \cdot 846153\ldots
\end{array}$$

The two sets of numerators, (1, 3, 4, 9, 10, 12) and (2, 5, 6, 7, 8, 11), have interesting derivations and properties. For instance, if a list is made of the squares of the natural numbers 1, 2, 3, . . ., and from these we subtract the largest multiple of thirteen that will leave a positive remainder, we have:

$$\begin{array}{cccccccccc}
1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & 81 & \ldots \\
 & & & 13 & 13 & 26 & 39 & 52 & 78 & \ldots \\
\hline
1 & 4 & 9 & 3 & 12 & 10 & 10 & 12 & 3 & \ldots
\end{array}$$

which provides a recurrent cycle (in a different order) of the numbers 1, 3, 4, 9, 10, 12, that is, the first set of numerators shown above.

Again, the two sets, which we will call respectively $A$ and $B$, have a curious internal property. Multiplying any two or more of the numbers of set $A$ together and then subtracting a suitable multiple of thirteen leaves a remainder which is one of the numbers in the set. Thus $(3 \times 12) - 26 = 10$, and $(3 \times 4 \times 9) - (8 \times 13) = 4$, and so on. Moreover, on applying the same procedure to members of set $B$ we again arrive at the numbers of set $A$, as follows $(2 \times 8) - 13 = 3$. On the other hand if a number from set $A$ is multiplied by one from set $B$ the outcome is a member of set $B$.

It would be impracticable to pursue this line of thought further until some experience of congruences and quadratic residues has been gained but it must occasion some surprise that there is a direct link between recurrent decimals and the square numbers.

(6) And finally to round off this chapter I am going to revert to a construction method which the reader might care to experiment with and/or find an explanation.

We see from Table 5 that 1/121 is equal to

$$\cdot\dot{0}08264462809917355371\dot{9}\ldots..$$

The following operations require no verbal description.

```
  8      = 8
  8 + 18 =  26
 26 + 18 =   44
 44 + 18 =    62
 62 + 18 =     80
 80 + 18 =      98
 98 + 18 =      116
116 + 18 =       134
134 + 18 =        152
152 + 18 =         170
170 + 18 =          188
188 + 18 =           206
206 + 18 =            224  etc.
           ------------------------
           826446280991735537190082 . . .

  1 + 18 =            19
 19 + 18 =           37
 37 + 18 =          55
 55 + 18 =         73
 73 + 18 =        91
 91 + 18 =      109
109 + 18 =     127
127 + 18 =    145
145 + 18 =   163
163 + 18 =  181
181 + 18 = 199  etc.
        ----------------------
        . . .0082644628099173553719
```

EXERCISES

1. What are the decimal equivalents of

   3/41, 7/41, 13/41, 29/41, and 30/41?

2. Find empirically some algorithm which generates the recurrent period of the fraction 1/441. (= $1/21^2$), namely

   ·002267573696145124716553287981859410430839 . . .

   This exercise might be expanded into a general search for algorithms among these periods. Anyone with a flair for empirical observation will find ample scope for ingenuity in this field.

# 4 ADDITIVE SERIES

(1) One of the most exciting things about experimenting with numbers is that one can so rapidly find oneself in strange and unfamiliar surroundings. And in such a situation there is little that can compete with the thrill of coming across some unexpected link with an apparently unrelated branch of mathematics.

A particular and most interesting example of this is to be found in a study of the additive series originated by Leonardo de Pisa, nowadays better known as Fibonacci. This series, first defined in the early part of the thirteenth century, is usually presented in the form 0, 1, 1, 2, 3, 5, 8, 13, . . ., each new term being the sum of the two preceding terms. In actual fact the fundamental properties of this important series would remain unchanged whatever integers were used to start it. Thus, observing the rule and giving any value we like to $a$, and $b$, the series becomes:

$a$, $b$, $(a + b)$, $(a + 2b)$, $(2a + 3b)$, $(3a + 5b)$, $(5a + 8b)$, etc.

For reasons which will be clarified later it will be found convenient to re-write the series in the form of two columns $A$ and $B$, the respective terms of which are determined by the following instructions:

$$A_{n+1} = A_n + B_n,$$
$$B_{n+1} = B_n + A_{n+1}.$$

Taking successive values from the above table and determining the decimal equivalents of the fractions $B_n/A_n$ and $(A_{n+1})/B_n$ it will be found that these both converge towards the value

1·6180339888 . . .,

thus,

89/55 = 1·61818 . . ., 144/89 = 1·61765 . . .
233/144 = 1·61806 . . ., 377/233 = 1·61798 . . .
610/377 = 1·61804 . . ., 987/610 = 1·61803 . . .

and so on.

**Table 6**

**The Reconstructed Fibonacci Series**

| *n* | *A* | *B* |  |
|---|---|---|---|
| 1 | 0 | 1 |  |
| 2 | 1 | 2 |  |
| 3 | 3 | 5 |  |
| 4 | 8 | 13 |  |
| 5 | 21 | 34 |  |
| 6 | 55 | 89 |  |
| 7 | 144 | 233 |  |
| 8 | 377 | 610 |  |
| 9 | 987 | 1597 |  |
| 10 | 2584 | 4181 | etc. |

We come now to a remarkable property of this series. The fractions $A_n/B_n$ and $B_n/(A_{n+1})$ get closer and closer, as $n$ increases, to 0·61803 . . . (for example 89/144 = 0·61805 . . .), while the fractions $(A_{n+1})/A_n$ and $(B_{n+1})/B_n$ approach 2·61803 . . ..

The Greeks knew this proportion (1·61803 . . .) as the Golden Ratio and made frequent use of it in their architecture and sculpture. It seems to have a curiously aesthetic attraction and many famous canvasses have dimensions closely approximating to adjacent members of the series. The ratio is now more commonly referred to as the Golden Section and is variously indicated by the Greek symbols for 'phi' or 'tau'.

It is the ratio of a diagonal to a side in a regular pentagon and of the radius of a circle to the side of an inscribed regular decagon. It forms the ratio between the number of clockwise and anti-clockwise spirals in the seed patterns of such flowers as sunflowers and in those of the areoles of globular cacti. It can be used to generate the logarithmic spiral governing the growth of sea and snail shells and the distribution of leaves around the stems of many plants, and at least one dedicated research worker claims to have correlated it to the ratio of the height of women's navels to their total stature.

In spite, or perhaps because, of the richly coloured applications that have been claimed for this innocent looking series it has come to be regarded more as a mathematical curiosity than as a subject for serious study and has received scant attention in most writings on the higher arithmetic. In what follows I hope to modify this impression and to show that there is a sound mathematical content in series of this form.

(2) First to deal with the fairly well-known properties of the Golden Ratio. Partly to avoid conflict with the adherents of 'phi' and 'tau', and partly to cope with the limitations of my typewriter, I shall use '$F$' to indicate 1·61803 . . ..

It is readily verified that $(1·618\ldots)^2 = 2·618\ldots$, and that $1/1·618\ldots = 0·618\ldots$. Thus $F$ is a number whose reciprocal is obtained by subtracting unity and which is squared by adding unity. Both of these statements, $1/F = (F - 1)$ and $F^2 = F + 1$ produce the quadratic equation

$$F^2 - F - 1 = 0$$

Solving this by normal algebraic procedure we obtain:

$$F = \frac{-b \pm \sqrt{(b^2 - 4ac)}}{2a} = (1 + \sqrt{5})/2 = 1·618\ldots.$$

It follows that $1/F = (\sqrt{5} - 1)/2 = 0·618\ldots$, and since $\sqrt{5}$ is irrational, that is its decimal part neither terminates nor recurs, then $F$ is also irrational.

Both $F$ and the series from which it is derived have strange properties. For instance, keeping one eye on Table 6, note the following relationships:

$$\begin{aligned}
2 \times 5 - 3^2 &= 2^2 - 1 \times 3 = 1\\
5 \times 13 - 8^2 &= 5^2 - 3 \times 8 = 1\\
13 \times 34 - 21^2 &= 13^2 - 8 \times 21 = 1\\
34 \times 89 - 55^2 &= 34^2 - 21 \times 55 = 1 \qquad \text{and so on.}
\end{aligned}$$

The reader may well find it interesting to search for other associations, perhaps using different starting numbers for '$A$' and '$B$', but I think it is safe to predict that he will find it difficult wholly to escape from the sequential integers of the series.

Even the ascending powers of $F$ cannot disengage themselves as will be seen from the following relationships,

$$\begin{aligned}
F &= F\\
F^2 &= F + 1\\
F^3 &= 2F + 1\\
F^4 &= 3F + 2\\
F^5 &= 5F + 3\\
F^6 &= 8F + 5\\
F^7 &= 13F + 8 \qquad \text{and so on.}
\end{aligned}$$

But perhaps the most unexpected property of this series emerges when the two numbers 1·61803 . . . and 2·61803 . . . are multiplied in turn by the natural numbers 1, 2, 3, 4, . . ., the fractional parts of the products being ignored. The first few pairs of numbers formed in this way are:

(1, 2), (3, 5), (4, 7), (6, 10), (8, 13), (9, 15), (11, 18),

and it can be shown that however far the operation is carried no integer is repeated and none omitted.

(3) References to the 'magical' properties of the Golden Section are often to be found in articles dealing with mathematical puzzles and paradoxes and it is often claimed, or at least implied, that it occupies an unique position in regard to the peculiarities which have just been mentioned. This may be true in some senses but let us return to our presentation of the Fibonacci series in two columns and try a slight change in its formulation.

The '*A*' and '*B*' columns will now be constructed according to the rules:

$$A_{n+1} = A_n + B_n$$
$$B_{n+1} = A_n + A_{n+1}$$

We then have,

**Table 7**

| $n$ | $A$ | $B$ |
|---|---|---|
| 1 | 0 | 1 |
| 2 | 1 | 1 |
| 3 | 2 | 3 |
| 4 | 5 | 7 |
| 5 | 12 | 17 |
| 6 | 29 | 41 |
| 7 | 70 | 99 |
| 8 | 169 | 239 |
| 9 | 408 | 577 |
| 10 | 985 | 1393 |
| 11 | 2378 | 3363 |
| 12 | 5741 | 8119 |
| 13 | 13860 | 19601 |
| . . . | . . . | . . . |

One of the advantages of using a two column presentation of such series will now become apparent; stretched out in a single line as Fibonacci's series is usually written it would be difficult to recognise this one as purely additive. However by its method of construction it most certainly is, and from an arithmetical point of view it is equally interesting.

Applying to the values in Table 7, the technique which provided the *F* number 1·61803 . . . and its derivatives we find that the ratio $B_n/A_n$ approaches, as $n$ increases, the limit 1·41421356237 . . ., which is of course the decimal expression of $\sqrt{2}$.

Furthermore the ratios $(A_{n+1})/A_n$ and $(B_{n+1})/B_n$, as $n$ increases, approach the value $\sqrt{2} + 1$, $(B_{n+1})/A_n$ gets nearer and nearer to $\sqrt{2} + 2$, and so on. Incidentally, these ratios and the general properties of this series are, as in the Fibonacci construction, quite unaffected by the choice of the two starting numbers.

This latter series also shares what seemed to be a property peculiar to the '*F*' numbers. Multiplying the values 1·4142 . . . and 3·4142 . . . successively by the whole numbers 1, 2, 3, 4, . . . and discarding the fractional parts of the products we again find a sequence of pairs of numbers which includes all the natural numbers without duplication. The first few of these pairs are:

(1, 3), (2, 6), (4, 10), (5, 13), (7, 17), (8, 20), (9, 23), . . .

and here we see that the differences between the numbers in brackets are successively 2, 4, 6, 8, etc.

(4) Striking as these properties and the relationships between the two series are, there is a still more remarkable connection to be noticed between them and some of the periods of the recurrent decimals examined in Chap. 3. Four examples from my own observations will be given and I have no doubt the reader will find this an exciting field for further research.

(*A*) If we take the original Fibonacci series, 0, 1, 1, 2, 3, 5, etc., and divide each term in turn by 10, 100, 1000, and so on, and then sum the results we have:

```
·0112358
       13
        21
         34
          55
           89
           144
            233
             377
              610
               987
               1597
               . . .
·011235955056179 . . . = 1/89 (see Table 3).
```

(*B*) If, on the other hand, the alternate terms of this series—as shown in column *A* of Table 6—are treated in the above manner we arrive at the following summation:

```
·0138
    21
     55
     144
      377
       987
       2584
        6765
        17711
         46368
         121393
          317811
           832040
           2178309
            5702887
            14930352
             39088169
             102334155
              . . .
·014084507042 . . .    = 1/71.
```

(*C*) Now we stated earlier—and this is easily demonstrated—that the ratio between successive terms of the Fibonacci series approaches *F* whatever integers are used to start the sequence. Again using the above process but this time starting with the numbers 5, and 26, and dividing the successive terms by $10^2$, $10^4$, $10^6$ etc., we now have:

```
·0526315788
          145
            233
              378
                611
                  989
                   1600
                     2589
                       4189
                        . . .
·0526315789473684210526 3 . . . = 1/19
```

(*D*) Turning now to (4, 3), in which a series producing the ratio 1·41421 . . . ($\sqrt{2}$) was described, it will be seen that this sequence of numbers also has its surprises. Taking alternate terms—that is the consecutive lines of column *A* in Table 7—and treating them as in (*A*) and (*B*) above we obtain the decimal equivalent of the fraction 1/79, thus:

```
·0125
    12
     29
      70
      169
       408
        985
        2378
         5741
         13860  and continuing,
          33461
           80782
           195025
            470832
            1136689
             2744210
              . . .
·01265822784810 . . .    = 1/79.
```

I think this link with the recurrent periods of 'prime denominator' fractions presents additive series in a new light and certainly there is scope here for some research.

### EXERCISES

1. Calculate $6F^2/5$ to five significant figures.

$$(F = 1{\cdot}61803\ldots)$$

2. What is the sum of the first $n$ Fibonacci numbers?

# 5 ONE ONE ONE ...... ONE

(1) In the previous chapters we have frequently run up against those numbers which belong to one or the other of the forms $10^n - 1$ or $10^n + 1$. Expressed in digital language these are respectively of the general types

$$9999\ldots 99 \text{ and } 1000\ldots 01.$$

We have seen that rapid checks of divisibility can easily be applied to the factors of such numbers and that they have an important bearing upon the structure of recurring decimals; for these and a variety of other reasons it will be of interest to examine them in greater detail and to discover some of their special properties and behaviour.

All integers of the form $A^n - 1$ are divisible by $A - 1$ and therefore in dealing with numbers of the form $10^n - 1$ it will be most convenient first to remove the factor 9 and concentrate upon the sequence 1, 11, 111, . . ., 111 . . . 1. In what follows such integers will be referred to as '*I*' numbers, and in particular $I_n$ will be used to indicate $(10^n - 1)/9$, or the integer 111 . . . 1 having $n$ digits. Thus, for example, $I_5 = 11111 = (10^5 - 1)/9$.

It will also be convenient to use a similar convention to describe integers of the form $10^n + 1$; these will be referred to as '*J*' numbers, the subscript again being equal to $n$. Thus $J_5$, or $10^5 + 1$ represents 100001, $n$ in this case being the number of zeros plus one.

By definition $I_n \times J_n = I_{2n}$ and in general it is easily seen that when $n$ is composite $I_n$ can always be resolved into at least two factors, as for example:

$$\begin{aligned} I_{12} &= 11 \times 10101010101 = 111 \times 1001001001 \\ &= 1111 \times 100010001 = 111111 \times 1000001 \end{aligned}$$

$I_n$ can therefore only be prime when $n$ is prime and indeed it is one of the most remarkable properties of both the '*I*' and '*J*' numbers that they seem to be extraordinarily free from primes. (I say 'seem' because the existing tests of primality become exceedingly difficult to apply when $n$ exceeds 37.)

$I_2$ (= 11) is certainly prime, $I_{19}$ is generally accepted to be prime, although I have not found any reference to a *positive* proof of this. On the other hand $I_{23}$ is still widely quoted as being prime in spite of a somewhat dubious ancestry and a proof of its composite character by D. H. Lehmer in 1927. Beyond this there are no more prime $I_n$'s up to, at least $n = 137$.

(2) One might expect that numbers constructed in such an orderly and regular fashion would exhibit some sort of pattern in the distribution of their factors. As we shall see later this is to a certain extent true but at first sight complete factorisation presents a chaotic picture.

The following Tables 8 and 9, list the factors of the smaller $I$ and $J$ numbers. I think these factors are all prime but am not completely certain about the large factors of $I_{25}$, and those of $J_n$ where $n = 20, 22$, and 23. Perhaps after studying the factorisation methods which will be described later some readers may find the subject interesting enough to try their hand at cracking these somewhat formidable numbers.

**Table 8**

**Factors of $I_n \left(= \dfrac{10^n - 1}{9}\right)$**

| $n$ | *Factors* |
|---|---|
| 2 | 11 (prime) |
| 3 | 3.37 |
| 4 | 11.101 |
| 5 | 41.271 |
| 6 | 3.7.11.13.37 |
| 7 | 239.4649 |
| 8 | 11.73.101.137 |
| 9 | 3.3.37.333667 |
| 10 | 11.41.271.9091 |
| 11 | 21649.513239 |
| 12 | 3.7.11.13.37.101.9901 |
| 13 | 53.79.265371653 |
| 14 | 11.239.4649.909091 |
| 15 | 3.31.37.41.271.2906161 |
| 16 | 11.17.73.101.137.5882353 |
| 17 | 2071723.5363222357 |
| 18 | 3.3.7.11.13.19.37.52579.333667 |
| 19 | 1111111111111111111 (thought to be prime) |
| 20 | 11.41.101.271.9091.99009901 |
| 21 | 3.37.43.239.1933.4649.10838689 |
| 22 | 11.11.23.4093.8779.21649.513239 |
| 23 | (Composite but factors not known) |
| 24 | 3.7.11.13.37.73.101.137.9901.99990001 |
| 25 | 41.271.1000010000100001000001 |
| 26 | 11.53.79.859.265371653.1058313049 |
| 27 | 3.3.3.37.757.333667.440334654777631 |
| 28 | 11.29.101.239.281.4649.909091.121499449 |
| 29 | 3191.16763.43037.62003.77843839397 |
| 30 | 3.7.11.13.31.37.41.211.241.271.2161.9091.2906161 |
| 32 | 11.17.73.101.137.353.449.641.1409.69857.5882353 |
| 34 | 11.103.4013.2071723.5363222357.21993833369 |
| 36 | 3.3.7.11.13.19.37.101.9901.52579.333667.999999000001 |
| 38 | 11.1111111111111111111.909090909090909091 |

Incidentally, $I_{38}$ is unique among the numbers listed above in that it is the only one, with $n$ even, that has *three* prime factors.

**Table 9**

**Factors of $J_n$ $(= 10^n + 1)$**

| $n$ | *Factors* |
|---|---|
| 1 | 11 (prime) |
| 2 | 101 (prime) |
| 3 | 7.11.13 |
| 4 | 73.137 |
| 5 | 11.9091 |
| 6 | 101.9901 |
| 7 | 11.909091 |
| 8 | 17.5882353 |
| 9 | 7.11.13.19.52579 |
| 10 | 101.99009901 |
| 11 | 11.23.4093.8779 |
| 12 | 73.137.99990001 |
| 13 | 11.859.1058313049 |
| 14 | 29.101.281.121499449 |
| 15 | 7.11.13.211.241.2161.9091 |
| 16 | 353.449.641.1409.69857 |
| 17 | 11.103.4013.21993833369 |
| 18 | 101.9901.999999000001 |
| 19 | 11.909090909090909091 |
| 20 | 73.137.9999000099990001 |
| 21 | 7.7.11.13.127.2689.459691.909091 |
| 22 | 89.101.1112470797641561909 |
| 23 | 11.47.139.2531.549797184491917 |
| 24 | 17.5882353.9999999900000001 |
| 25 | 11.251.5051.9091.78875943472201 |

(3) Of course, if we are content to express these numbers by, at most, only two factors a much more regular pattern emerges, as exemplified in the following breakdown of the $J$ numbers.

| | | | |
|---|---|---|---|
| $J_2$ | 101 | $J_3$ | 11.91 |
| $J_4$ | 10001 | $J_5$ | 11.9091 |
| $J_6$ | 101.9901 | $J_7$ | 11.909091 |
| $J_8$ | 100000001 | $J_9$ | 11.90909091 |
| $J_{10}$ | 101.99009901 | | etc. |

In fact these numbers containing only the digits 0, 1, and 9, arranged in various patterns offer in themselves an interesting subject for research; one set in particular provides an excellent example of the dangers of drawing hasty conclusions in enquiries of this kind. Taking in sequence one of the factors of $J_{3n}$ (or $I_{6n}$) we have:

| | | |
|---|---|---|
| $J_3$ | 91 | composite |
| $J_6$ | 9901 | prime |
| $J_9$ | 999001 | composite |
| etc. | 99990001 | prime |
| | 9999900001 | composite |
| | 999999000001 | prime |
| | 99999990000001 | composite |
| | 9999999900000001 | prime |
| | 999999999000000001 | composite |

One might be tempted to infer that the next number in the sequence (99999999990000000001) is prime but fortunately as it must be a factor of $I_{60}$ it is not difficult to prove that it is composite.

Since 60 contains the factors 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, it follows that $I_{60}$ must contain all the factors appearing in the numbers $I_2$, $I_3$, $I_4$, . . . $I_{30}$, namely, (11), (3.37), (101), (41.271), (7), (9091), (9901), (31.2906161), (99009901), and (211.241.2161). It is easy to see that if these factors are multiplied together the product must have more than forty digits and hence $I_{60}$ cannot have a single prime factor of twenty digits.

The number 99999999990000000001 must therefore have at least one of the above primes as a factor.

(4) It will be seen from Tables 8 and 9, or for that matter readily deduced from first principles, that divisors of $I_n$ numbers are also divisors of $I_{mn}$ where $m$ is one of the natural numbers 1, 2, 3, . . .. Consequently when dealing with the $I$ and $J$ numbers we need really only be concerned with those primes which appear as divisors *for the first time*. These will recur in all multiples of $n$ and further research on numbers of this form will be made easier by abstracting the primary factors and presenting them in tabular form as in the following Table 10.

Table 10

**Primary Factors of $I_n$**

| $n$ | *Factors* |
|---|---|
| 2 | 11 |
| 3 | 3.37 |
| 4 | 101 |
| 5 | 41.271 |
| 6 | 7.13 |
| 7 | 239.4649 |
| 8 | 73.137 |
| 9 | 333667 |
| 10 | 9091 |
| 11 | 21649.513239 |
| 12 | 9901 |
| 13 | 53.79.265371653 |
| 14 | 909091 |
| 15 | 31.2906161 |
| 16 | 17.5882353 |
| 17 | 2071723.5363222357 |
| 18 | 19.52579 |
| 19 | 1111111111111111111 |
| 20 | 99009901 |
| 21 | 43.1933.10838689 |
| 22 | 23.4093.8779 |
| 23 | not known |
| 24 | 99990001 |
| 25 | 100001000010000100001 |
| 26 | 859.1058313049 |
| 27 | 757.440334654777631 |
| 28 | 29.281.121499449 |
| 29 | 3191.16763.43037.62003.77843839397 |
| 30 | 211.241.2161 |
| 31 | 2791.*N* |
| 32 | 353.449.641.1409.69857 |
| 33 | 67.*N* |
| 34 | 103.4013.21993833369 |
| 35 | 71.*N* |
| 36 | 999999000001 |
| 37 | 2028119.*N* |

This table provides a number of working examples of one of the most important theorems in the Theory of Numbers and at the same time an insight into a puzzling feature of the varying periods of recurring decimals.

In the first place, remembering that factors of $I_n$ are also factors of $I_{nm}$ we see that:

7 is a factor of $I_6$
11 is a factor of $I_{10}$
13 is a factor of $I_{12}$
17 is a factor of $I_{16}$
and so on.

And generally, when $n$ is prime it is a divisor of $I_{n-1}$.

Bearing in mind how the $I_n$ numbers are constructed this is seen to be a particular example of 'Fermat's Theorem' which states that if $p$ is prime and $N$ is not a multiple of $p$, then $N^{p-1} - 1$ is divisible by $p$ exactly. This theorem is of fundamental utility in the exploration of numbers; proofs, depending usually either on binomial expansion or congruence theory, will not be given here as they are to be found in almost every textbook on Algebra.

The table also serves to illustrate the following lesser—but still important—theorems. Here again the proofs, which though not difficult depend upon a sequence of lemmas, are left to the formal textbooks. (For instance, *Advanced Algebra*, Barnard and Child Macmillan & Co. Ltd.)

(1) If $n$ is an odd prime, every prime factor of $N^n - 1$ which is not a divisor of $N - 1$ is of the form $2kn + 1$.

(2) If $p$ is a prime factor of $N^n + 1$ it is also a factor of $N^d + 1$ where $d$ is the greatest common divisor of $n$ and $\frac{1}{2}(p - 1)$.

(3) If $n$ is a prime, every odd prime factor of $N^n + 1$ which is not a divisor of $N + 1$ is of the form $2kn + 1$.

(4) If $n$ is a prime, every prime factor of $N^{n^x} - 1$ which is not a divisor of $N^{n^{x-1}} - 1$ is of the form $kn^x + 1$.

(5) Every prime factor of $N^{2^n} + 1$ is of the form $2^{n+1}. k + 1$.

These theorems are of value in limiting the choice of possible factors of both $I$ and $J$ numbers and as we shall see later it is possible to narrow the field still further.

(5) Before pursuing this line however, it will be of interest to note a connection between recurring decimals and Table 10. Referring back to Table 3 and its following paragraph we recall that the recurrent period of the decimal form of $1/p$ contains a number of digits which is equal either to $p-1$ or to some divisor of $p-1$. Thus 1/7, ($=\cdot\dot{1}4285\dot{7}$) has six digits whilst 1/53, ($=\cdot\dot{0}18867924528\dot{3}$) has $52/4=13$ digits. At first sight the period lengths appear to be decided in an entirely random manner.

But the factors of $I_n$ are in effect the factors of 999 . . . 9 (having $n$ 9's) and the periods of recurring decimals are exact divisors of numbers of this kind. In consequence the reciprocals of the *factors* shown in Table 10 have the corresponding $n$ number of digits in their recurring period. Thus both 1/41 ($=\cdot\dot{0}243\dot{9}$), and 1/271 ($=\cdot\dot{0}036\dot{9}$) have five-digit cycles, 1/7, and 1/13, six-digits, and so on. Furthermore in the whole infinity of the natural numbers there can only be one whose reciprocal has exactly 2, 4, 10, . . . 19, . . . 36, etc., digits.

(6) The factorisation of $I$ numbers presents a challenge which is difficult to resist and although we shall deal with general methods of factorisation later this is an appropriate point to mention some aids which can be applied to these numbers in particular. Unfortunately it is outside the scope of this book to discuss the theory of Quadratic Residues (that is, the remainders left after subtracting a given prime or its multiples from the sequence of square numbers) but one of its consequences must be mentioned in this context.

Numbers which have a Quadratic Residue of 10 are of the general form $40k+1, 3, 9, 13, 27, 31, 37, 39,$ whilst those with a Q.R. of $-10$ are of the form $40k+7, 11, 17, 19, 21, 23, 29, 33.$ It can be shown that primary factors of $I_n$ (i.e. $n$ odd) must be of the first form whilst those of $J_n$ are of the second. This, I am afraid, will have to be taken on trust as far as formal proof is concerned but the factors given in Table 10 and a subsequent table (12) will show a practical confirmation of these statements.

The important thing is that we now have two independent 'forms' of factors of these numbers and these can be combined to give a much more economical approach to their factorisation.

To take a specific example let us examine the possible factors of $I_7$ (= 1,111,111). These must be of one or more of the forms $40s+1, 3, 9, 13,$ etc., and at the same time of the form $14t+1$: equating

these forms in turn we have:

($A$) $14t+1=40s+1$, and hence $7t=20s$. This equation is satisfied when $t=20, 40, \ldots 20k$. Substituting, we have $14(20k)+1=280k+1$.

($B$) $14t+1=40s+3$, thus $7t=20s+1$, which is satisfied when $t=3, 23, 43, \ldots 20k+3$. Then $14(20k+3)+1=280k+43$.

Continuing in this way it is not difficult to determine that the factors of $I_7$ must be of one of the forms

$$280k+1, 43, 71, 169, 197, 239, 253, 267.$$

There are 168 odd primes less than the square root of $I_7$ but by using this elimination process one factor (239) is disclosed at the fourth trial. The other factor (4649) is equal to $(280\times16)+169$.

The following table has been constructed on these lines and should prove useful to anyone intending to pursue the subject.

### Table 11

### 'Forms' of Factors of $I_n$

| $n$ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5 | $40k+1$, | 31. | | | | | | |
| 7 | $280k+1$, | 43, | 71, | 169, | 197, | 239, | 253, | 267. |
| 9 | $360k+1$, | 37, | 163, | 199, | 253, | 271, | 289, | 307. |
| 11 | $440k+1$, | 67, | 89, | 111, | 133, | 199, | 243, | 397. |
| 13 | $520k+1$, | 27, | 53, | 79, | 157, | 209, | 313, | 391. |
| 15 | $120k+1$, | 31. | | | | | | |
| 17 | $680k+1$, | 239, | 307, | 409, | 443, | 477, | 511, | 613. |
| 19 | $760k+1$, | 39, | 77, | 191, | 267, | 533, | 609, | 723. |
| 21 | $840k+1$, | 43, | 169, | 253, | 547, | 631, | 757, | 799. |
| 23 | $920k+1$, | 73, | 231, | 277, | 323, | 369, | 507, | 599. |
| 25 | $200k+1$, | 151. | | | | | | |
| 27 | $1080k+1$, | 163, | 271, | 649, | 757, | 919, | 973, | 1027. |
| 29 | $1160k+1$, | 117, | 523, | 639, | 813, | 871, | 929, | 987. |
| 31 | $1240k+1$, | 187, | 249, | 311, | 373, | 559, | 683, | 1117. |
| 33 | $1320k+1$, | 67, | 133, | 199, | 397, | 529, | 991, | 1123. |
| 35 | $280k+1$, | 71. | | | | | | |
| 37 | $1480k+1$, | 519, | 667, | 889, | 963, | 1037, | 1111, | 1333. |
| 39 | $1560k+1$, | 79, | 157, | 391, | 547, | 1093, | 1249, | 1483. |
| 41 | $1640k+1$, | 83, | 329, | 493, | 1067, | 1231, | 1477, | 1559. |
| 43 | $1720k+1$, | 173, | 431, | 517, | 603, | 689, | 947, | 1119. |
| 45 | $360k+1$, | 271. | | | | | | |
| 47 | $1880k+1$, | 283, | 471, | 1129, | 1317, | 1599, | 1693, | 1787. |
| 49 | $1960k+1$, | 197, | 883, | 1079, | 1373, | 1471, | 1569, | 1667. |

(7) Even with the aids described above, however, the factorisation of $I_n$ and $J_n$ becomes extremely difficult as $n$ increases and there is scope here for further research into links between possible prime factors and $n$. As a start in this direction it might be worth while to note that although $I_n$ is not always composite it is obvious that every prime is a factor of *some* $I_n$ (see the opening remarks on recurring decimals in Chap. 3). It may therefore be of interest to approach the problem, empirically, from the rear.

In the following table the odd primes up to 1051 are listed, together with the $n$ values of $I_n$ for which they are factors. Thus, for example, it will be seen that when $p = 41$, the corresponding

### Table 12

### Values of $n$ for which $I_n$ is a multiple of $p$

| $p$ | $n$ | $p$ | $n$ | $p$ | $n$ | $p$ | $n$ | $p$ | $n$ |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 163 | 81 | 367* | 366 | 593* | 592 | 823* | 822 |
| 7* | 6 | 167* | 166 | 373 | 186 | 599 | 299 | 827 | 413 |
| 11* | 2 | 173 | 43 | 379* | 126 | 601 | 300 | 829* | 276 |
| 13 | 6 | 179* | 178 | 383* | 382 | 607* | 202 | 839 | 419 |
| 17* | 16 | 181* | 180 | 389* | 388 | 613 | 51 | 853 | 213 |
| 19* | 18 | 191 | 95 | 397 | 99 | 617* | 88 | 857* | 856 |
| 23* | 22 | 193* | 192 | 401 | 200 | 619* | 618 | 859* | 26 |
| 29* | 28 | 197 | 98 | 409 | 204 | 631 | 315 | 863* | 862 |
| 31 | 15 | 199 | 99 | 419* | 418 | 641 | 32 | 877 | 438 |
| 37 | 3 | 211* | 30 | 421* | 140 | 643 | 107 | 881 | 440 |
| 41 | 5 | 223* | 222 | 431 | 215 | 647* | 646 | 883 | 441 |
| 43 | 21 | 227 | 113 | 433* | 432 | 653 | 326 | 887* | 886 |
| 47* | 46 | 229* | 228 | 439 | 219 | 659* | 658 | 907 | 151 |
| 53 | 13 | 233* | 232 | 443 | 221 | 661* | 660 | 911 | 455 |
| 59* | 58 | 239 | 7 | 449 | 32 | 673* | 224 | 919 | 459 |
| 61* | 60 | 241 | 30 | 457* | 152 | 677 | 338 | 929 | 464 |
| 67 | 33 | 251* | 50 | 461* | 460 | 683 | 341 | 937* | 936 |
| 71 | 35 | 257* | 256 | 463* | 154 | 691* | 690 | 941* | 940 |
| 73* | 8 | 263* | 262 | 467 | 233 | 701* | 700 | 947 | 473 |
| 79 | 13 | 269* | 268 | 479 | 239 | 709* | 708 | 953* | 952 |
| 83 | 41 | 271 | 5 | 487* | 486 | 719 | 359 | 967* | 322 |
| 89 | 44 | 277 | 69 | 491* | 490 | 727* | 726 | 971* | 970 |
| 97* | 96 | 281 | 28 | 499* | 498 | 733 | 61 | 977* | 976 |
| 101* | 4 | 283 | 141 | 503* | 502 | 739* | 738 | 983* | 982 |
| 103* | 34 | 293 | 146 | 509* | 508 | 743* | 742 | 991 | 495 |
| 107 | 53 | 307 | 153 | 521 | 52 | 751 | 125 | 997 | 166 |
| 109* | 108 | 311 | 155 | 523 | 261 | 757 | 27 | 1009 | 252 |
| 113* | 112 | 313* | 312 | 541* | 540 | 761 | 380 | 1013 | 253 |
| 127* | 42 | 317 | 79 | 547 | 91 | 769 | 192 | 1019* | 1018 |
| 131* | 130 | 331* | 110 | 557 | 278 | 773 | 193 | 1021* | 1020 |
| 137* | 8 | 337* | 336 | 563 | 281 | 787 | 393 | 1031 | 103 |
| 139* | 46 | 347 | 173 | 569 | 284 | 797 | 199 | 1033* | 1032 |
| 149* | 148 | 349* | 116 | 571* | 570 | 809 | 202 | 1039 | 519 |
| 151 | 75 | 353* | 32 | 577* | 576 | 811* | 810 | 1049 | 524 |
| 157 | 78 | 359 | 179 | 587 | 293 | 821* | 820 | 1051* | 1050 |

value of $n$ is 5, indicating that 41 is an exact divisor of $I_5$, or 11,111.

(It is worth noting that when $p$ is of one of the forms $40k + 7$, 11, 17, 19, 21, 23, 29, 33, then $n$ is always an even number and consequently $p$ is also a factor of $J_{n/2}$.)

(A still more important observation can be divided into two parts:

(*a*) When $p$ is of the above form, $40k + 7$, 11, 17, etc.—marked thus * in the table—then $n$ is equal to $(p - 1)$ divided by an *odd* number. For example, $(17 - 1)/1 = 16$; $(73 - 1)/9 = 8$, etc.

(*b*) When $p$ is of the form $40k + 1$, 3, 9, 13, 27, 31, 37, 39, $n$ is equal to $(p - 1)$ divided by an *even* number, as $(31 - 1)/2 = 15$; $(173 - 1)/4 = 43$.)

| | | |
|---|---|---|
| Note also: | $p =$ 493121, | $n =$ 67 (Brillhart) |
| | 497867 | 89 (Brillhart) |
| | 18797 | 127 (McCullough) |
| | 80173 | 131 (McCullough) |
| | 2467 | 137 (McCullough) |
| | 12517 | 149 (McCullough) |
| | 12671 | 181 (McCullough) |
| | 52009 | 197 (McCullough) |

# 6 PATTERNS AMONG THE 'ONES'

(1) We saw in the last chapter that when $n$ is composite it is always a simple matter to find at least two factors of $I_n$ and although it may not be easy to say whether these are prime or composite the process does reduce the magnitude of the numbers to be tested. The examples given employed only the digits 0, 1 and 9, but other factor patterns can be found when $n$ is of certain specific 'forms'.

For instance, we have:

(*A*) When $n = 3k$,

$$I_3 = 3 \cdot 37$$
$$I_6 = 33 \cdot 3367$$
$$I_9 = 333 \cdot 333667$$
$$I_{12} = 3333 \cdot 33336667 \quad \text{and so on.}$$

(*B*) When $n = 6k$,

$$I_6 = 91 \cdot 1221$$
$$I_{12} = 9901 \cdot 11222211$$
$$I_{18} = 999001 \cdot 111222222111$$
$$I_{24} = 99990001 \cdot 1111222222221111 \quad \text{etc.}$$

(*C*) When $n = 4k + 2$,

$$I_2 = 11$$
$$I_6 = 91 \cdot 1221$$
$$I_{10} = 9091 \cdot 122221$$
$$I_{14} = 909091 \cdot 12222221$$
$$I_{18} = 90909091 \cdot 1222222221 \quad \text{etc.}$$

Associated with the above the following curiously regular 'irregularities' are worth noting:

3367 = 37.91
33336667 = 37.900991
3333366667 = 37.90090991
33333336666667 = 37.900900990991
3333333366666667 = 37.90090090990991
33333333336666666667 = 37.900900900990990991
3333333333336666666666667 = 37.9009009009099099 0991 etc.

A more intriguing partition of factors of certain $I_n$ numbers is to be found in a system which is not completely consistent. When $n = 5k$, $I_n$ can be divided into the following pairs of factors:

| $n$ | |
|---|---|
| 5 | 41.271 |
| 10 | 451.2463661 |
| 15 | 4551.24414658561 |
| 20 | 45551.243926831707561 |
| 25 | $455551.2439048780731709756 + \underline{55555}$ |
| 30 | 4555551.243902682927073170975 61 |
| 35 | 45555551.2439024634146365853660975 61 |
| 40 | 455555551.24390244146341465853658560975 61 |
| 45 | 4555555551.2439024392682926831707317075609 7561 |
| 50 | $45555555551.24390243904878048780731707317097560975 6 +$<br>$\underline{5555555555}$ |

and so on, with every $I_{25k}$ failing to conform to the pattern. (Note that $455551 = 41^2 . 271$.)

This peculiarity is not confined to members of the $I_{5k}$ clan as can be seen by making a similar partition when $n = 7$.

| $n$ | |
|---|---|
| 7 | 239.4649 |
| 14 | 2629.4226364059 |
| 21 | 26529.418828870711 7159 |
| 28 | 265529.418451887029707154 8159 |
| 35 | 2655529.4184142259832640167405858159 |
| 42 | 26555529.41841046025146443556485397489581 59 |
| 49 | $265555529.418410083682012552301673640209205025104 6 +$<br>$\underline{7777777}$ |

and so on. Again, $265555529 = 239^2 . 4649$.

(2) Similar investigations into the construction of the $J$ numbers must, I am sure, be equally rewarding and I recommend this as a project for the reader. In case however, the large numbers with which we have been dealing have been a little over-powering this chapter will be rounded off with a few observations which do not demand quite so much muscular mathematics.

It may seem hardly worth remarking that since 41, for instance, is a divisor of 11111, it must also divide 4111111, but it is perhaps not quite so obvious that it is also a factor of 4000001, 400000000001, etc. Similarly 37 is an exact divisor of 31117, 31111117, . . . and 30007, 30000007, etc.

The reasons for these 'phenomena' are easily discovered but what follows is not so obvious. Since, for example, 4649 is a factor of $I_7$ it is also an exact divisor of 40000000649, 46000000049, 46400000009 and all other members of the same pattern containing $7k$ zeros (or for that matter $7k$ 'ones').

(3) We have seen that the $I$ and $J$ numbers can present problems of interest and considerable complexity and that the determination of their prime or composite character is in general extremely difficult; on the other hand their construction by additive methods is, as might be expected, not only simple but open to a variety of approaches. Some of these relating to the $I$ numbers are given below; the reader may find it diverting to extend these examples or perhaps to find similar expressions for the $J$ numbers.

$$(A)\quad \begin{aligned} 1 &= (6-5)/1 = (7-4)/3 = (8-3)/5 = (9-2)/7\ldots \\ 11 &= (6^2-5^2)/1 = (7^2-4^2)/3 = \ldots \\ 111 &= (56^2-55^2)/1 = (57^2-54^2)/3 = \ldots \\ 1111 &= (556^2-555^2)/1 = (557^2-554^2)/3 = \ldots \quad \text{and so on.} \end{aligned}$$

$$(B)\quad \begin{aligned} 11 &= (10^2-1)/9 \\ 111 &= (60^2-51^2)/9 \\ 1111 &= (560^2-551^2)/9 \\ 11111 &= (5560^2-5551^2)/9 \\ 111111 &= (55560^2-55551^2)/9 \quad \text{etc.} \end{aligned}$$

(*C*)

$$\begin{aligned}
11 &= ((9 \times 9) + 7)/8 \\
111 &= ((98 \times 9) + 6)/8 \\
1111 &= ((987 \times 9) + 5)/8 \\
11111 &= ((9876 \times 9) + 4)/8 \\
\dots & \quad \dots \\
111111111 &= ((98765432 \times 9) + 0)/8 \\
1111111111 &= ((987654321 \times 9) - 1)/8
\end{aligned}$$

(*D*)

$$\begin{aligned}
11 &= 1 \times 9 + 2 \\
111 &= 12 \times 9 + 3 \\
1111 &= 123 \times 9 + 4 \\
11111 &= 1234 \times 9 + 5 \\
\dots & \quad \dots \\
111111111 &= 12345678 \times 9 + 9 \\
1111111111 &= 123456789 \times 9 + 10
\end{aligned}$$

(*E*)

$$\begin{aligned}
11 &= 6^2 - 5^2 = 4^2 - 5 = 3^2 + 2 \\
1111 &= 56^2 - 45^2 = 34^2 - 45 = 33^2 + 22 \\
111111 &= 556^2 - 445^2 = 334^2 - 445 = 333^2 + 222 \\
11111111 &= 5556^2 - 4445^2 = 3334^2 - 4445 = 3333^2 + 2222 \text{ etc.}
\end{aligned}$$

(*F*)

$$\begin{aligned}
111 &= 6^2 + 75 = 7^2 + 62 \\
11111 &= 66^2 + 6755 = 67^2 + 6622 \\
1111111 &= 666^2 + 667555 = 667^2 + 666222 \\
111111111 &= 6666^2 + 66675555 = 6667^2 + 66662222 \quad \text{etc.}
\end{aligned}$$

(*G*)

$$\begin{aligned}
11 &= (3 \times 4) - 1 \\
1111 &= (33 \times 34) - 11 \\
111111 &= (333 \times 334) - 111 \\
11111111 &= (3333 \times 3334) - 1111 \quad \text{etc.}
\end{aligned}$$

(*H*)

$$\begin{aligned}
1 &= 1 \\
11 &= 2 + 9 \\
111 &= 3 + (3 \times 9) + 9^2 \\
1111 &= 4 + (6 \times 9) + (4 \times 9^2) + 9^3 \\
11111 &= 5 + (10 \times 9) + (10 \times 9^2) + (5 \times 9^3) + 9^4 \quad \text{etc.}
\end{aligned}$$

Here, in effect, $I_n$ has been expressed in the scale of nine, and it will be seen that the coefficients are those of the binomial expansion of $(1 + x)^n$.

If should be noted—though I hope without surprise—that if the sequences of numbers defined by $2^n \pm 1$ are expressed in the scale of 2, they become:

| | $2^n - 1$ | | $2^n + 1$ | | |
|---|---|---|---|---|---|
| $n$ | $S_{10}$ | $S_2$ | $S_{10}$ | $S_2$ | |
| 1 | 1 | 1 | 3 | 11 | |
| 2 | 3 | 11 | 5 | 101 | |
| 3 | 7 | 111 | 9 | 1001 | |
| 4 | 15 | 1111 | 17 | 10001 | etc. |

And finally, although it is outside the intended scope of this book I cannot resist adding this little gem for the entertainment of those readers who are familiar with the operation of determinants:

$$\begin{vmatrix} I_n & I_{n+1} & I_{n+2} \\ I_{n+1} & I_{n+2} & I_{n+3} \\ I_{n+2} & I_{n+3} & I_{n+4} \end{vmatrix} = 0$$

In expanded, and far less picturesque form, this becomes (for compactness putting $o, p, q, r,$ in the place of $n + 1, n + 2,$ etc.):

$$I_n(I_p \times I_r - I_q{}^2) + I_o(I_q \times I_p - I_r \times I_o) + I_p(I_o \times I_q - I_p{}^2) = 0$$

Testing this for $n = 1$, for example, we then have:

$$\begin{aligned}
&(111.11111 - 1111^2) + 11(1111.111 - 11111.11) + \\
&\quad 111(11.1111 - 111^2) = (1233321 - 1234321) + \\
&\quad 11(123321 - 122221) + 111(12221 - 12321) = \\
&\quad -1000 + 11(1100) + 111(-100) = -1000 + \\
&\qquad 12100 - 11100 = 0.
\end{aligned}$$

### EXERCISES

1. What factors are common to both 1001001001 and 100010001?
2. Why must 90909091 be composite?
3. What are the factors of 33336667?

# 7 PRIME NUMBERS

(1) Primes, those integers which have no factors other than themselves and unity, have fascinated and tortured amateurs and some of the greatest mathematical minds in history alike for centuries. And the total of our knowledge of them is still disappointingly small.

We know that the primes continue indefinitely—that there is no 'largest' prime; we know that no algebraic expression can be written that generates only primes. We know an analytic formula which will tell us how many primes to expect less than any given number, but only to a very rough approximation, and a procedure giving an exact figure at the expense of extremely laborious computations. We know of some expressions in $x$ (variable) that contain infinitely many primes but these are mostly trivial and though we suspect others they have not yet been proved.

A few tests which distinguish between prime and composite numbers are known but they are difficult to apply to integers of even moderate size. And, broadly speaking, that's about the lot.

Oddly enough, in spite of what has been said, we can compose strings of consecutive integers which are composite for as many terms as we like to specify although to be frank this is of little value in the theory of primes.

Having said this let us look at some of the intriguing ways in which the problem of the primes has been attacked.

Proof of the infinity of the primes dates back at least to Euclid whose reasoning is a model for all time of succinct elegance. Suppose, he argued, that $P$ is the largest prime: then if $P$ and all the smaller primes are multiplied together and 1 is added to the product, then this new number cannot be exactly divisible by $P$ or any lesser prime. It must therefore either be itself a prime or divisible by some prime greater than $P$; in either case there is a prime greater than $P$.

Although there can be no formula which produces only primes—

proof of this may be found in any college algebra—there are some expressions which have an almost magical facility up to a point. For instance, the sequence $p + 0, p + 2, p + 6, . . .$ (which is the same thing as $p + n^2 - n, n$ taking the successive values $1, 2, 3, . . .$) obviously becomes equal to $n^2$ when $n = p$ but up to this point, when $p = 3, 5, 11, 17,$ and 41 we have:

| $p = 3$ | 5 | 11 | 17 | 41 | | |
|---|---|---|---|---|---|---|
| 5 | 7 | 13 | 19 | 43 | 347 | 1163 |
| 9 | 11 | 17 | 23 | 47 | 383 | 1231 |
| | 17 | 23 | 29 | 53 | 421 | 1301 |
| | 25 | 31 | 37 | 61 | 461 | 1373 |
| | | 41 | 47 | 71 | 503 | 1447 |
| | | 53 | 59 | 83 | 547 | $1523 = 39^2 + 2$ |
| | | 67 | 73 | 97 | 593 | $1601 = 40^2 + 1$ |
| | | 83 | 89 | 113 | 641 | $1681 = 41^2$ |
| | | 101 | 107 | 131 | 691 | |
| | | 121 | 127 | 151 | 743 | |
| | | | 149 | 173 | 797 | |
| | | | 173 | 197 | 853 | |
| | | | 199 | 223 | 911 | |
| | | | 227 | 251 | 971 | |
| | | | 257 | 281 | 1033 | |
| | | | 289 | 313 | 1097 | |

All these integers except the terminal ones are prime. It is difficult to believe that it is only by chance that these sequences pick their steps so daintily without once treading on a composite number but so far no one has been able to find a prime greater than 41 which produces a further series of this kind.

Other expressions are occasionally 'discovered', but these arise from the fact that $n$ can be given negative values or be replaced by, for example $(n - 40)$, and in this way it is possible to devise a confusing array of 'different' formulae. Thus, for instance, we can write:

$$n^2 + 3n + 43$$
$$n^2 + 5n + 47$$
$$n^2 + 7n + 53 \quad \text{and so on,}$$

or $$n^2 - 79n + 1601$$

or $$n^2 + an + \frac{(a^2 + 163)}{4}. \quad \text{(when } a \text{ is odd).}$$

All these formulae produce exactly the same sequence of prime numbers as the original.

(2) A fundamental property of prime numbers is conveyed in the statement, 'If $n$ is any integer and $p$ is a prime, then $n^p - n$ is exactly divisible by $p$.'

Over 2000 years ago the Chinese knew this to be true in the special case of $n = 2$, but nowadays the above is known as 'Fermat's (lesser) Theorem'. Fermat first declared the general form—without proof—in a letter to a fellow mathematician in October 1640. Removing the factor $n$ we obtain the form in which the theorem is more commonly stated, namely; 'If $p$ is a prime number, and $n$ an integer not a multiple of $p$, then $n^{p-1} - 1$ is exactly divisible by $p$.'

The first formal proof of this theorem was given by Leibniz (1646–1716). In an age in which algebraic symbolism was in a primitive state and which consequently required propositions of this sort to be argued out verbally the proof must have presented formidable difficulty: today it is disposed of in a few lines in any school algebra.

The theorem permiates the Theory of Numbers like a mycelium but unfortunately its converse cannot be relied upon as a test of primality without some highly sophisticated refinements.

Another important theorem connected with prime numbers is that known as 'Wilson's'. This, reminiscent of Euclid's proof of the infinity of primes, states that if, *and only if*, $p$ is a prime, then

$$(2.3.4.5. \ldots .(p-1)) + 1$$

is exactly divisible by $p$. ($2.3.4.5. \ldots .n$ is known as 'factorial $n$' and is written $n!$). In most Algebra schoolbooks the theorem is stated thus:

If $p$ is a prime number, then $(p-1)! + 1$ is divisible by $p$. Contrary to Fermat's this theorem is only true when $p$ is prime as can easily be shown. For if $p$ has a factor, say $m$, then $m$ is less than $p$ and must therefore divide $(p-1)!$. The same goes for its other factor and hence neither of them can be divisors of $(p-1)! + 1$.

Factorial numbers increase very rapidly even for quite small values of $n$, as can be seen from the table in the Appendix, and consequently Wilson's theorem has no value at present as a test of primality. On the other hand it has some interesting consequences. For instance it is not difficult to derive from it that if $p$ and $p + 2$ are both prime then

$$2(p-1)! + 1 \text{ is divisible by } p + 2.$$

Anything bearing on 'pairs' of primes such as 5/7, 11/13, 17/19, 59/61, 115301/115303, 100004561/100004563, 1000000009649/1000000009651, etc., is worth noting since the theory of these numbers has scarcely been scratched and it is not even known whether they continue indefinitely.

Perhaps if some technique for dealing with large factorials can be developed, comparable say with that now available for use against the converse of Fermat's theorem, Wilson's might yet disclose new horizons.

Although this property of factorials does not appear to provide an effective weapon against the primes factorials do enable us to make the most fantastic demands upon composite numbers. Lists of prime numbers display irregularly spaced gaps indicating strings of consecutive composite integers; these appear to be randomly distributed and increase in length as the numbers become larger. Nevertheless it would require a long list of primes and quite a laborious search before we could find say, fifty numbers without a single prime among them. And yet if we were to make the impossible-looking demand for a million consecutive composite numbers factorials provide the answer immediately. It is only necessary to write $1000001! \pm 2, \pm 3, \ldots \pm 1000001$, and we have two sets of numbers which fulfil the requirement. For since $n!$ is divisible by $2, 3, 4, \ldots$, adding or subtracting $2, 3, 4$, etc., will not affect this property and all integers within the intervals proscribed must therefore be composite.

Of course this is a most profligate means of ensuring that such a demand is met. For instance to make sure of say, twenty-four consecutive composite numbers it is necessary to start with 25! or 15511210043330985984000000 whereas all the integers between 3137 and 3163 are composite.

(3) A most interesting and far-reaching generalisation of Fermat's Theorem was first announced by Euler in 1760. In this he began by examining those integers which are 'relatively prime' to one another, that is which have no common factors. Thus, for example, 7, 8, 9, 25, are all relatively prime though three of them are composite.

Now any given number $m$ has just so many integers less than $m$ which are relatively prime to it; the number of such integers is denoted by $\phi(m)$—Euler's function. When $m$ is a prime then clearly $\phi(m) = m - 1$, but with $m$ composite there is some counting to be done. Thus when $m = 14$, three are six integers prime to $m$, namely, 1, 3, 5, 9, 11, 13, and therefore $\phi(14) = 6$.

Euler's generalisation in effect substitutes $\phi(m)$ for $(p - 1)$ in Fermat's statement that $n^{p-1} - 1$ is divisible by $p$, and extends the theorem to include *all* values of $m$. We now have, "$n^{\phi(m)} - 1$ is exactly divisible by $m$, provided only that $n$ is relatively prime to $m$".

Taking again the above example, $m = 14; \phi(m) = 6$, the theorem shows that for $n = 1, 3, 5, 9, 11, 13; n^6 - 1 = 14k$.

Thus: $3^6 - 1 = 728 = 14.52$
$5^6 - 1 = 15624 = 14.1116$
$9^6 - 1 = 531440 = 14.37960$ etc.

It should be noted that $n$ can be *any* integer that is relatively prime to $m$, and thus we have for instance,

$$17^6 - 1 = 24137568 = 14.1724112.$$

(Note. Since 7 is not a member of the set, $7^6 - 1 = 117648 \neq 14k$.)

Although quite incidental to the above ideas it will be of interest to observe that if any two or more of the integers 1, 3, 5, 9, 11, 13, are multiplied together and the product divided by 14, the remainder is always a member of the set.

For example, $5.13 = 65 = (4.14) + 9$,
$3.11 = 33 = (2.14) + 5$, etc.

This is a property of all sets of integers which are relatively prime to a given number.

Methods of determining $\phi(m)$ for any value of $m$ can be stated simply. Their derivations and proofs will not, however, be given here because they are most elegantly presented by the use of congruence techniques. (See H. Davenport's *The Higher Arithmetic.*) The basic principle can be described as follows:

Let $m = a^r . b^s . c^t \ldots$, where $a$, $b$, and $c$, etc., are prime factors.

Then $\phi(m) = m(1 - 1/a)(1 - 1/b)(1 - 1/c) \ldots$. (Note that $r$, $s$, $t$, etc. do not enter into the calculation.) Thus, for example, when $m = 40 = 2^3 \times 5, \phi(40) = 40(1 - 1/2)(1 - 1/5) = 40 \times 1/2 \times 4/5 = 16$.

In the following list (Table 13) all the values of $\phi(m)$ for $m < 400$ have been tabulated. Before looking at its practical use as an aid to factorisation the following observations can be made; all but the final one can be proved and can be used to extend the table as required.

(*a*) Every value of $\phi(m)$ is an even number.
(*b*) When $m$ is prime, then $\phi(m) = m - 1$.
(*c*) When $m$ is odd, then $\phi(m) = \phi(2m)$.
(*d*) When $m$ is even, then $\phi(2m) = 2.\phi(m)$.
(*e*) When $m$ is odd yet not a multiple of three, (i.e. of the form $6k \pm 1$), then $\phi(3m) = \phi(4m) = \phi(6m)$.
(*f*) When $m$ is a square number, say $a^2$, then $\phi(a^2) = a.\phi(a)$.
(*g*) All values of $\phi(m)$ are repeated at least once. This is a conjecture which has not yet been proved.

The practical use to which this function can be put is perhaps best illustrated by taking an example from Table 13. It will be seen, for instance, that $\phi(399) = 216$. (See the end of the last line in the table.) Since 10 is prime to 399, we can therefore state that $10^{216} - 1$, $(= 9.I_{216})$ is a multiple of 399, $(= 3.7.19)$. Looking further up the table it will be seen that 216 also appears as a function of 351, 333, 327, 259, and 247. Factorising these numbers we obtain the 'new' primes 13, 37, 109 and it is then possible to state that $I_{216}$ is a multiple of $3.7.13.19.37.109$. (The reader might find a gentle exercise in checking these findings back to the original definition of Euler's function.) It will be noted that Fermat could not have helped here, since 217 is not prime.

(4) It was recognised early in mathematical history that no formula could be found that excluded all composite numbers but there still remained conjectures about 'forms' of numbers which (*a*) provided

## Table 13

### Euler's Function $\phi(m)$

($\phi(m)$ is the number of integers less than, and relatively prime to $m$)

| $m$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | — | — | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 |
| 10 | 4 | 10 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 |
| 20 | 8 | 12 | 10 | 22 | 8 | 20 | 12 | 18 | 12 | 28 |
| 30 | 8 | 30 | 16 | 20 | 16 | 24 | 12 | 36 | 18 | 24 |
| 40 | 16 | 40 | 12 | 42 | 20 | 24 | 22 | 46 | 16 | 42 |
| 50 | 20 | 32 | 24 | 52 | 18 | 40 | 24 | 36 | 28 | 58 |
| 60 | 16 | 60 | 30 | 36 | 32 | 48 | 20 | 66 | 32 | 44 |
| 70 | 24 | 70 | 24 | 72 | 35 | 40 | 36 | 60 | 24 | 78 |
| 80 | 32 | 45 | 40 | 82 | 24 | 64 | 42 | 56 | 40 | 88 |
| 90 | 24 | 72 | 44 | 60 | 46 | 72 | 32 | 96 | 42 | 60 |
| 100 | 40 | 100 | 32 | 102 | 48 | 48 | 52 | 106 | 32 | 108 |
| 110 | 40 | 72 | 48 | 112 | 36 | 88 | 56 | 72 | 58 | 96 |
| 120 | 32 | 110 | 60 | 80 | 60 | 100 | 36 | 126 | 64 | 84 |
| 130 | 48 | 130 | 40 | 108 | 66 | 72 | 64 | 136 | 44 | 138 |
| 140 | 48 | 92 | 70 | 120 | 48 | 112 | 72 | 84 | 72 | 148 |
| 150 | 40 | 150 | 72 | 96 | 60 | 120 | 48 | 156 | 78 | 104 |
| 160 | 64 | 132 | 54 | 162 | 80 | 80 | 82 | 166 | 48 | 156 |
| 170 | 64 | 108 | 84 | 172 | 56 | 120 | 80 | 116 | 88 | 178 |
| 180 | 48 | 180 | 72 | 120 | 88 | 144 | 60 | 160 | 92 | 108 |
| 190 | 72 | 190 | 64 | 192 | 96 | 96 | 84 | 196 | 60 | *198* |
| 200 | 80 | 132 | 100 | 168 | 64 | 160 | 102 | 132 | 96 | 180 |
| 210 | 48 | 210 | 014 | 140 | 106 | 168 | 64 | 180 | 108 | 444 |
| 220 | 220 | 80 | 192 | 72 | 222 | 96 | 120 | 112 | 226 | 72 |
| 230 | 88 | 120 | 112 | 232 | 72 | 184 | 116 | 156 | 96 | 238 |
| 240 | 64 | 240 | 110 | 162 | 120 | 168 | 80 | 216 | 120 | 164 |
| 250 | 100 | 250 | 72 | 220 | 126 | 128 | 128 | 256 | 84 | 216 |
| 260 | 96 | 168 | 130 | 262 | 80 | 208 | 108 | 176 | 132 | 268 |
| 270 | 72 | 270 | 128 | 144 | 136 | 200 | 88 | 276 | 138 | 180 |
| 280 | 96 | 280 | 92 | 282 | 140 | 144 | 120 | 240 | 96 | 272 |
| 290 | 112 | 192 | 144 | 292 | 84 | 232 | 144 | 180 | 148 | 264 |
| 300 | 80 | 252 | 150 | 200 | 144 | 240 | 96 | 306 | 120 | 204 |
| 310 | 120 | 310 | 96 | 312 | 156 | 144 | 156 | 316 | 104 | 280 |
| 320 | 128 | 212 | 132 | 288 | 108 | 240 | 162 | 216 | 160 | 276 |
| 330 | 80 | 330 | 164 | 216 | 166 | 264 | 96 | 336 | 156 | 224 |
| 340 | 128 | 300 | 108 | 294 | 168 | 176 | 172 | 346 | 112 | 348 |
| 350 | 120 | 216 | 160 | 352 | 116 | 280 | 176 | 192 | 178 | 358 |
| 360 | 96 | 342 | 180 | 220 | 144 | 288 | 120 | 366 | 176 | 240 |
| 370 | 144 | 312 | 120 | 273 | 160 | 184 | 184 | 336 | 108 | 378 |
| 380 | 144 | 252 | 190 | 382 | 128 | 240 | 192 | 252 | 192 | 388 |
| 390 | 96 | 352 | 168 | 260 | 196 | 312 | 120 | 396 | 198 | 216 |

only primes, and (*b*) contained an infinity of primes. Perhaps the best known guess in class (*a*) was that made by Fermat. His formula for primes, to this day known as 'Fermat Numbers' or $F_n$ was $2^{2^n} + 1$, where $n = 1, 2, 3, \ldots$.. This expression clearly produced primes for $n = 1, 2, 3, 4$, and there the matter stood until in 1732 Euler showed that $F_5 = 4{,}294{,}967{,}297 = 641 . 6{,}700{,}417$.

Nearly 150 years elapsed before $F_6$ was cracked.

$$F_6 = 18{,}446{,}744{,}073{,}709{,}551{,}617 = 274{,}177 \times 67{,}280{,}421{,}310{,}721.$$

Many more composite numbers of this form have since been found but not, so far as I know, any more primes. Thus $F_n$ for $n = 7, 8, 10, 13, 14, 16$, is known to be composite, and the following factors have been found:

$F_9$ is divisible by $37.2^{16} + 1$
$F_{11}$ is divisible by $(39.2^{13} + 1)(119.2^{13} + 1)$
$F_{12}$ is divisible by $(7.2^{14} + 1)(397.2^{16} + 1)$
$F_{15}$ is divisible by $579.2^{21} + 1$
$F_{18}$ is divisible by $13.2^{20} + 1$
$F_{23}$ is divisible by $5.2^{25} + 1$
$F_{36}$ is divisible by $5.2^{39} + 1$
$F_{38}$ is divisible by $3.2^{41} + 1$
$F_{73}$ is divisible by $5.2^{75} + 1$

(To appreciate the size of these numbers the last *factor*, $5.2^{75} + 1$ is equal to 188,894,659,314,785,808,547,841.)

These numbers increase at a fabulous rate and yet, thanks to highly sophisticated techniques developed in the last half century, it is now known that the almost incomprehensible number $F_{1945}$ is divisible by $5.2^{1947} + 1$.

It would seem that Fermat's conjecture has somersaulted and one should now ask whether any primes beyond $F_4$ exist at all.

(5) Although not strictly belonging to either of the above classes, no discussion of the primes would be complete without some mention of the 'Mersenne' numbers. Mersenne, a contemporary of Fermat (1588–1648), studied the numbers $2^p - 1$ ($p$—prime) and in 1644 made a statement to the effect that the only values of $p$ that make $2^p - 1$ a prime are 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. (Being nobody's fool one assumes that he added, or implied, $p < 260$.)

These numbers do not increase with anything like the rapidity of Fermat's, but nevertheless the factorisation of the intervening numbers must have presented, in those days, a most formidable problem. It was not until the end of the nineteenth century that $M_{61}$ was proved to be prime and this was followed by Cole's demonstration in 1903 that $M_{67}$ was composite (193,707,721 × 761,838,257,287). More primes of this form, $p > 257$, have been found since, the largest to date (1968) being $2^{11213} - 1$.

Mathematical fortune-telling on meagre empirical evidence is no longer a popular pastime but it must not be forgotten that the efforts to prove or disprove these two wild guesses have probably contributed more to the development of factorisation methods and tests of primality than any other problems in the Theory of Numbers.

In class (*b*) we have a rather different situation. Since, for instance, $4n \pm 1$ and $6n \pm 1$ contain respectively all the odd numbers and all those not divisible by three, these progressions obviously contain all the primes. Simple as it may seem the proof that each of these four progressions contains an infinity of primes requires some effort and any amateur who completes the set can call himself a mathematician.

Dirichlet proved (1837) that the series $an + b$ ($a$ relatively prime to $b$) generates an infinite number of primes and it is conjectured—as yet without proof—that the same applies to the series $n^2 + 1$. There is, of course, no limit to propositions of this kind but when it comes to proof it is difficult to find a point of contact with the few known properties of the primes.

### EXERCISES

1. For what values of $n$ is $n^8 - 1$ divisible by 20?
2. Use Table 13 to find four prime factors of $5^{12} - 1$.
3. What is the value of $\phi(402)$?

# 8 PRIME NUMBERS (Part 2)

(1) In this chapter some of the lesser known surmises and observations concerning the primes will be described.

One of the most curious of these is Euler's proposed test for the primality of integers of the form $N = 4n + 1$ which end in 3 or 7, or more concisely those of the form $20m + 13, + 17$. (These integers represent one quarter of all the odd numbers.) The criterion then runs:

'Let $R$ be the remainder after subtracting from $2N$ the next smaller square which ends in 5, namely $(5n)^2$. Then to $R$ add cumulatively the numbers $100(n - 1), 100(n - 3), 100(n - 5), \ldots$ and so on. If among these sums, including $R$ itself, there occurs a *single* square number, then $N$ is either a prime or is divisible by this square. If, on the other hand, two or more squares, or none, occur then $N$ is composite.'

The following four examples will serve to disentangle these unusual and somewhat confusing instructions.

(*A*) $N = 637$.
$$\begin{aligned} 2N &= 1274\\ 35^2 &= \underline{1225} = (5n)^2, \text{ so } n = 7.\\ R &= \phantom{00}49 \end{aligned}$$

Then $R, (R + 600), (R + 400), (R + 200) = 49, 649, 1049, 1249$. In this set the only square is 49, and therefore $N$ is either prime or is divisible by 49. In fact $637 = 49 \cdot 13$.

(*B*) $N = 2437$.
$$\begin{aligned} 2N &= 4874\\ 65^2 &= \underline{4225} \text{ therefore } n = 13\\ R &= \phantom{0}649 \end{aligned}$$

The sequence then becomes, 649, 1849, 2849, 3649, 4249, 4649, 4849. Here the only square number is 1849 and since 2437 is clearly not divisible by 1849 then it is prime.

(*C*) $N = 2303$.
$$\begin{aligned} 2N &= 4606\\ 65^2 &= \underline{4225} \quad n = 13\\ R &= \phantom{0}381 \end{aligned}$$

Sequence—381, 1581, 2581, 3381, 3981, 4381, 4581. Since this does not contain a square, $N$ is composite.

(*D*) $N = 2117$.
$$\begin{aligned} 2N &= 4234\\ 65^2 &= \underline{4225} \quad n = 13\\ R &= \phantom{000}9 \end{aligned}$$

Sequence—9, 1209, 2209, 3009, 3609, 4009, 4209. Of these numbers 9 and 2209 are square and therefore 2117 is composite ($= 29 \cdot 73$).

One might go on for a long time testing numbers of these two forms at random before coming across an anomaly. In fact where the test indicates that an integer is composite it is invariably true but unfortunately some composite numbers appear amongst those it picks as prime. The first few of these are 153, 333, 477, 657, 833, . . ., and are in general those integers which are multiples of primes of one of the forms $(20k + 13)$ and $(20k + 17)$ and also of one or more of the squares of 3, 7, 9, 11, 23, 27, . . . (i.e. $(20m + 3, 7, 9, 11)^2$).

(Assuming that the first step in any test for primes would be the elimination of 3, 7, 11, 13, as possible factors the first error would not occur until we reached $8993 = 17 \,.\, 23^2$, a truly remarkable achievement.)

Euler's test for primes of the above forms can therefore be polished by the further provision that any integer appearing as a prime must again be tested for divisibility by the numbers $(20m + 3, 7, 9, 11)^2$. In passing it might be of interest to note that the numbers $13^2 \,.\, 17$, $13^2 \,.\, 37$, $13^2 \,.\, 57, \ldots$ have sequences which include *three* squares, whilst $3^2 \,.\, 13$, $7^2 \,.\, 13$, $9^2 \,.\, 13$, $11^2 \,.\, 13, \ldots$ provide the cases where there is *one* square which divides $N$.

As far as I know no one has put forward anything comparable as a test for the other three forms of odd numbers and this most peculiar approach to the theory of primes—with such a master as its sponsor—might well initiate a rewarding project for some amateur.

(2) The following miscellaneous criteria for primes are given without references; they have been gathered much as one picks blackberries and I cannot say with certainty that all of them have been proved.

They should, however, give some idea of the concentrated effort and the diversity of approach which has been directed upon these fascinating and elusive members of our number system. Perhaps some of them will provoke a renewed attack. In what follows the symbol (*if*) will be used to indicate the expression 'if, and only if'.

(*a*) A number is prime (*if*) it is *not* expressible in the form $ab + xy$ when $a, b, x, y$, are positive integers such that $a + b = x - y$.

(*b*) A number $p$ is prime (*if*) it occurs $(p - 1)$ times in the $(p - 1)$th set where the first set is 1, 2, 1; the second set is 1, 3, 2, 3, 1—formed by inserting between each two terms of the preceding set their sum—the third 1, 4, 3, 5, 2, 5, 3, 4, 1, and so on.

(*c*) If $n$ is an odd number then $4n + 1$ is prime (*if*) it is a factor of $(2^{2n} + 1)/5$.

(*d*) If $p$ is a prime of the form $4k + 1$ then $2p + 1$ is also a prime (*if*) it exactly divides $(2^p + 1)/3$.

(*e*) If $p$ is a prime of the form $4k - 1$ then $2p + 1$ is also a prime (*if*) it exactly divides $2^p - 1$.

(*f*) If $p$ is an odd prime then the integral part of $(\sqrt{5} + 2)^p - 2^{p+1}$ is exactly divisible by $20p$.

(*g*) A number of the form $6n + 1$ is prime (*if*) $n$ cannot be expressed in either of the forms $6xy + x + y$, or $6xy - x - y$.

(*h*) A number of the form $6n - 1$ is prime (*if*) $n$ is not of the form $6xy + x - y$.

(*i*) If $p$ and $q$ are different primes then $p^{q-1} + q^{p-1} - 1$ is exactly divisible by $pq$.

(*j*) At least four primes lie between the squares of two consecutive primes $(>3)$.

(*k*) If $4n - 1$ and $8n - 1$ are both primes, then $2^{4n-1} - 1$ is a multiple of $8n - 1$.

(*l*) (*If*) $p$ is prime then $1 + 1/2 + 1/3 + \ldots 1/(p - 1)$ is exactly divisible by $p$.

(*m*) Given that $s$ and $c$ are respectively the arithmetic means of the squares and cubes of all the numbers less than and relatively prime to $n$, then $n^3 = 6ns - 4c$.

(*n*) Between any two primes there is an odd number of composite integers.

(3) Although nobody nowadays searches for a formula which will generate nothing but prime numbers it is still reasonable to ask 'what is the number of primes (say $P(x)$) less than a given integer $x$?'. Most surprisingly one answer was given in 1896 by Hadamard and de la Vallée Poussin independently, both men in or about their thirtieth year. It was to the effect that $P(x)$ approaches the value $x/\log_e x$ as $x$ tends to infinity.

This intrusion of Analysis—which deals with continuous functions and might be called the science of approximation—into a branch of mathematics concerned exclusively with the whole numbers was almost as revolutionary as the introduction of the minus sign into primitive arithmetic.

Of course for some limited values of $x$, $P(x)$ can be determined by an actual count, and the following lists may be worth noting for reference.

| | Number of primes |
|---|---|
| 0 – 1000 | 168 |
| 1000 – 2000 | 135 |
| 2000 – 3000 | 127 |
| 3000 – 4000 | 120 |
| 4000 – 5000 | 119 |
| 5000 – 6000 | 114 |
| 6000 – 7000 | 117 |
| 7000 – 8000 | 107 |
| 8000 – 9000 | 110 |
| 9000 – 10000 | 112 |

On a more extended scale we have (excluding 1, and 2) the number of primes less than

| | |
|---|---|
| 10 = | 3 |
| 100 = | 24 |
| 1000 = | 168 |
| 10000 = | 1229 |
| 100000 = | 9592 |
| 1000000 = | 78498 |
| 10000000 = | 664579 |
| 100000000 = | 5761455 |
| 1000000000 = | 50847478 |

(4) Finally a word on large primes. About sixteen years ago $2^{127}-1$, a number of some forty digits, held the record. Shortly afterwards $180(2^{127}-1)^2+1$ (about 83 digits) was proved prime. Since then we have had $2^p-1$ where $p = 521, 607, 1279, 2203$, and $2281$, this last containing 686 digits.

For a time it was thought by some that $2^q-1$ was prime when $q$ is a Mersenne prime but it has recently been shown that $2^{2^{13}-1}-1$ $(= 2^{8191}-1)$ is composite. And now there is this fabulous prime $2^{11213}-1$, employing 3376 digits.

Even this may have been surpassed by the time these notes appear.

# 9 AN INTRODUCTION TO DIOPHANTINE EQUATIONS

(1) Equations involving two or more unknowns which require solutions in integers or rational fractions date back to Diophantus of Alexandria in about the third or fourth century A.D. It has taken almost all the intervening time—some fifteen centuries—to bring these problems under control of some sort and even now there still remains the question of whether $x^n + y^n = z^n$, for $n$ greater than 2 has any solution.

Linear Diophantine equations can be expressed in the form $ax \pm by = c$, in which $a$, $b$, and $c$ are given and it is required to find integral values of $x$ and $y$.

We are all familiar with the type of popular mathematical puzzle exemplified by the following: A farmer pays £7 each for sheep and £12 each for calves. (I wouldn't know whether these are realistic prices today.) If he buys some of each for a total bill of £71, how many sheep and calves has he acquired?

Taking the number of sheep and calves to be respectively $x$ and $y$, we then have the equation $7x + 12y = 71$. It is to be understood of course that at the end of the transaction the animals are to be alive and running about on all four legs.

The standard school-book treatment of such a problem proceeds as follows:

$$7x + 12y = 71 \qquad (1)$$

Dividing by the smaller coefficient (7) we have,

$$x + y + 5y/7 = 10 + 1/7$$

or

$$x + y + (5y - 1)/7 = 10 \qquad (2)$$

Since $x$ and $y$ are integers then $(5y - 1)/7$ must be an integer and consequently $(15y - 3)/7$ is also an integer. (Here a multiplier is chosen which will make the coefficient of $y$ differ from a multiple of 7 by unity.)

$$\begin{aligned}\text{Now } (15y-3)/7 &= 2y + y/7 - 3/7\\ &= 2y + (y-3)/7\end{aligned}$$

As before it follows that $(y-3)/7$ is an integer and equal, say to $n$. Then $y - 3 = 7n$ or $y = 7n + 3$ (3)
Substituting this in (2) we have:

$$x + 7n + 3 + (35n + 15 - 1)/7 = x + 12n + 5 = 10$$

or $$x = 5 - 12n.$$

For $x$ to have a positive value $n$ must be zero and we have $x = 5$, and from (2) $y = 3$.

(2) Now there is a much simpler method of arriving at the above result. The algorithm may take a little space to describe but, once understood it is much quicker and more reliable in dealing with equations having large coefficients of $x$ and $y$.

Taking again the above example we re-write the equation thus: $7x = 71 - 12y$. (This is not really necessary but it helps with the explanation.) Divide the coefficients on the right by 7 and note down the remainders, i.e. $1(c)$ and $-5(b)$. (Remember the general equation is $ax + by = c$.) Set down the numbers 1, 2, 3, . . . $(a-1)$, or in this case

1, 2, 3, 4, 5, 6

Multiply each of these by the '$b$' coefficient, namely 5, to give 5, 10, 15, 20, 25, 30. Divide each of these by 7 and list the remainders thus:

5, 3, 1, 6, 4, 2

Note that the '$c$' coefficient, namely 1, is at the third position and write $y = 3$. (As easy as that) $x = 5$ is easily found by substitution.

The process is far simpler to apply than to describe and as a further example of the power of this method we ask 'What are the smallest integers which will satisfy the equation

$$11x + 127y = 1{,}067{,}723\,?\text{'}$$

Rewriting we have $11x = 1067723 - 127y$. Dividing by 11 the remainders are 8, 6. Then

1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

And, multiplying by 6 and subtracting multiples of 11—

6, 1, 7, 2, 8, 3, . . .

Since 8 is at the fifth position then $y = 5$, and by substitution $x = 97008$.

$$\begin{aligned}\text{Check: } 11 \times 97008 &= 1067088\\ 5 \times 127 &= \underline{\phantom{106}635}\\ &\phantom{=}\ 1067723\end{aligned}$$

(3) For equations of higher degree the problem becomes more difficult and although some types are amenable to treatment there is in fact as yet no general technique for determining even whether a solution is possible or not.

In the case of equations describing the so called Pythagorean right angled triangles we are on familiar and well trodden ground. These are triangles of sides $x$, $y$, and (hypoteneuse) $z$, and the problem is to find solutions of the equation $x^2 + y^2 = z^2$, $x$, $y$, $z$, being integers and having no factors in common.

The general solution can be reached by the following reasoning—I give this in full because it indicates the best known approach to the more difficult problems in this terrain:

(1) $x$ and $y$ cannot both be even, for then $z$ would also be even.
(2) $x$ and $y$ cannot both be odd for then $x^2 + y^2$ would be of the form $4n + 2$ which is never a square.

Suppose then that $x$ is odd and $y$, even. We can now write the equation $x^2 + 4t^2 = z^2$ or, $4t^2 = (z + x)(z - x)$.

But $x$ and $z$ are odd and therefore $z + x$, and $z - x$ are both even. Putting $z + x = 2s$ and $z - x = 2r$ we then have $4t^2 = 4sr$, or $t^2 = rs$.

Also $(z + x) + (z - x) = 2s + 2r$ or $z = r + s$ and similarly $x = s - r$.

Since $x$ and $z$ are relatively prime then so are $r$ and $s$. In consequence the equation $t^2 = rs$ requires that $r$ and $s$ are *each* perfect squares, say $r = n^2$ and $s = m^2$. Then $t = mn$ and it follows that

$$x = m^2 - n^2;\ y = 2mn;\ z = m^2 + n^2.$$

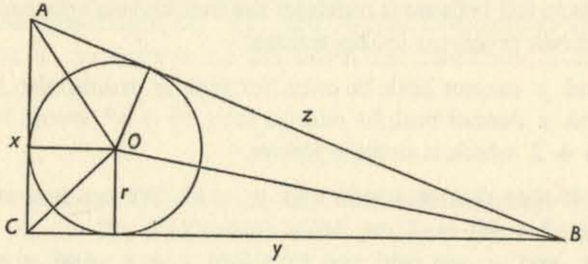
Even so $m$ and $n$ must obey certain conditions. Thus $m$ is greater than $n$ so that $x$ is positive; $m$ and $n$ must have no common factor or it would be shared by $x, y, z$; $m$ and $n$ must not both be odd for then $x$ and $z$ would both be even.

With these reservations in mind it is possible to tabulate as many solutions—in integers—of the equation $x^2 + y^2 = z^2$ as we wish.

For instance the first few are:

| $m$ | $n$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| 2 | 1 | 3 | 4 | 5 |
| 3 | 2 | 5 | 12 | 13 |
| 4 | 3 | 7 | 24 | 25 |
| 4 | 1 | 15 | 8 | 17 |
| 5 | 4 | 9 | 40 | 41 |
| 5 | 2 | 21 | 20 | 29 |
| 6 | 5 | 11 | 60 | 61 |
| 6 | 1 | 35 | 12 | 37 |

The above general solution to the Pythagorean equation has been well documented but there is a geometrical consequence to this which is perhaps not so well known. Given a right angled triangle whose sides and hypoteneuse can be expressed in integers we consider the radius of the inscribed circle.



The area of $\Delta ABC = x/2y = \Delta s\ AOB + BOC + COA$. Therefore $x/2y = \frac{1}{2}rz + \frac{1}{2}ry + \frac{1}{2}rx = \frac{1}{2}r(x + y + z)$ and $r = xy/(x + y + z)$.

If now we replace $x, y, z$ by their equivalents in $m$ and $n$ we have

$$r = \frac{(m^2 - n^2) \,.\, 2mn}{m^2 - n^2 + 2mn + m^2 + n^2}$$
$$= n(m - n)$$

Since both $m$ and $n$ are integers then $r$, the radius of the inscribed circle is also always an integer. In particular when $x = 3, y = 4, z = 5$, then $r = 1$.

### EXERCISES

1. Solve $5x + 9y = 1001$, for $x$ and $y$.
2. If in the equation $x^2 + y^2 = z^2$ we give $z$ the value of 26, what are the corresponding values of $x$ and $y$?

# 10 SOME OBSERVATIONS ON $X^n$

(1) In a broad sense experiments are of two kinds. Those which are made with the object of confirming or disproving a theoretical idea, and those whose sole purpose is that of gathering information. Of the two the latter can usually be expected to provide more opportunities of excitement than the former (unless of course the theory happens to be particularly novel and one's own).

Experiments designed to tell us how numbers behave under certain specific conditions nearly always produce something of interest if they are carried far enough. And in the world of numbers it is indeed remarkable how little initial data is needed to start a train of successive observations.

Let us take as a starting point, for example, one of the simplest properties of integers in the scale of ten. 'All powers of 10 end with the "units" digit 0.' (Incidentally all powers of $x$ in the scale of $x$ do the same but we shall confine ourselves to the everyday system here.) I am sure that no reader will require a formal proof of this. Nor will he need telling that all powers of 5, or for that matter of any number of the form $10k + 5$, end in 5 and that those of 6 end with a 6. The same thing holds for numbers terminating in 1 and it is easily seen that the even powers of $10k + 9$ end in 1 and the odd powers in 9.

Having made these observations it is natural to ask next what happens to the 'units' digits of powers of the remaining numbers $10k + 2, 3, 4, 7,$ and 8. Since we are only concerned at the moment with the final digits it is a simple matter to construct a table without calculating out the powers in full. For instance the units digits of the powers of 2 are 2, 4, 8, 6, 2, 4, etc., those of 3 are 3, 9, 7, 1, 3, and so on. In fact it is quickly seen that the terminal digits of the powers of all the natural numbers repeat themselves after, at most, a cycle of four digits.

**Table 14a**

**Terminal digits of $x^n$**

| $x$ | $n = 1$ | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 8 | 6 | 2 |
| 3 | 3 | 9 | 7 | 1 | 3 |
| 4 | 4 | 6 | 4 | 6 | 4 |
| 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 7 | 9 | 3 | 1 | 7 |
| 8 | 8 | 4 | 2 | 6 | 8 |
| 9 | 9 | 1 | 9 | 1 | 9 |

Having produced this table, what can be learnt from it? For a start there are four immediate observations which can be made.

(*A*) All the odd powers of any number $x$ may end in any of the digits 0, 1, 2, 3, . . . 9.

(*B*) $x^2$, $x^6$, and in general $x^{4n+2}$ can only end with the digits 0, 1, 4, 5, 6, and 9.

(*C*) $x^{4n}$ is restricted to endings of 0, 1, 5, 6.

(*D*) The even powers of any number can never terminate with the digits 2, 3, 7, or 8.

Much more information, however, can be squeezed out of this table. From at least the time of Fermat and Mersenne, numbers of the general form $x^n \pm 1$ have been the object of much study and speculation particularly in their connection with prime numbers. Although the table has no direct bearing on the primes it does enable us to sweep a wide area free from one class of composite numbers.

Since all integers ending in 0 or 5 are divisible by 5 then clearly the addition of unity to those powers of $x$ which have endings of 4 or 9 will make the resulting numbers composite (i.e. multiples of 5). Similarly, subtracting one from powers ending in 1 or 6 will have the same result.

Thus $2^2 + 1, 2^6 + 1, \ldots 2^{4+2} + 1$,

and $2^4 - 1, 2^8 - 1, \ldots 2^{4k} - 1$, are all divisible by 5.

Multiples of five are of course easily discernible when expressed in integers but this simple table enables us to list all such multiples which are of the general form $x^n \pm 1$ in the following specific algebraic statements:

$$\begin{array}{ll}
(10m + 2)^{4k} - 1, & (10m + 2)^{4k+2} + 1, \\
(10m + 3)^{4k} - 1, & (10m + 3)^{4k+2} + 1, \\
(10m + 4)^{2k} - 1, & (10m + 4)^{2k+1} + 1, \\
(10m + 6)^{k} \ - 1, & (10m + 7)^{4k+2} + 1, \\
(10m + 7)^{4k} - 1, & (10m + 8)^{4k+2} + 1, \\
(10m + 8)^{4k} - 1, & (10m + 9)^{4k+1} + 1. \\
(10m + 9)^{4k} - 1. &
\end{array}$$

(2) Now in considering the terminal (i.e. units) digits of $x^n$ we have, in effect, been concerned only with the remainders left after division by ten. It will be reasonable to continue with a similar examination of the 'digital roots' of the powers of the natural numbers; these are of course the remainders left after division by nine.

The corresponding table is quite simple to construct; as before it is not necessary to calculate the actual powers of $x$ since if $x = 9r + a$, then $x^2 = 9s + a^2$, $x^3 = 9t + a^3$, etc. Consequently we need only multiply the digital root of $x$ successively by $a$.

For example when $x = 7$, the digital roots of $x, x^2, x^3, \ldots$ are found thus: 7, $7 \cdot 7 = 49$ ($D.R. = 4$), $7 \cdot 4 = 28$ ($D.R. = 1$) and so on. In this manner we arrive at Table 14b which again is quite general and repeats itself cyclically when extrapolated either vertically or horizontally.

Since all numbers having the digital roots 3, 6, and 9 are divisible by three, we can use this table to sieve out another set of composite values of $x^n \pm 1$.

We see, for example that the digital roots of $2^1, 2^3, 2^5, 2^7$, etc., are always one of the digits 2, 5, 8, and that those of $2^2, 2^4, 2^6, 2^8$, etc., are either 1, 4, or 7. It follows therefore that 3 is always a factor of both

$$2^{2k+1} + 1 \text{ and } 2^{2k} - 1.$$

**Table 14b**

**Digital Roots of $x^n$**

| $x$ | $n = 1$ | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 8 | 7 | 5 | 1 | 2 |
| 3 | 3 | 9 | 9 | 9 | 9 | 9 | 9 |
| 4 | 4 | 7 | 1 | 4 | 7 | 1 | 4 |
| 5 | 5 | 7 | 8 | 4 | 2 | 1 | 5 |
| 6 | 6 | 9 | 9 | 9 | 9 | 9 | 9 |
| 7 | 7 | 4 | 1 | 7 | 4 | 1 | 7 |
| 8 | 8 | 1 | 8 | 1 | 8 | 1 | 8 |
| 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 |

Proceeding on these lines and generalising as before we are able then to make a list of all the values of $x^n \pm 1$ which are multiples of 3. Thus:

$$\begin{array}{ll}
(9m + 2)^{2k} - 1, & (9m + 2)^{2k+1} + 1, \\
(9m + 4)^{k} \ - 1, & (9m + 5)^{2k+1} + 1, \\
(9m + 5)^{2k} - 1, & (9m + 8)^{2k+1} + 1. \\
(9m + 7)^{k} \ - 1, & \\
(9m + 8)^{2k} - 1. &
\end{array}$$

(3) These two tables, extremely simple both in construction and appearance, contain a surprising amount of information, some of which is not easy to uncover by ordinary algebraic processes. To take an elementary example let us assume we are searching for primes among numbers of the form $2^n + 1$. Table 14b tells us that $2^{2k+1} + 1$, an expression containing all the *odd* powers of 2, is divisible by 3, whereas it is seen from Table 14*a* that $2^{4k+2} + 1$, or $2^{2,6,10,\text{etc}} + 1$, is always a multiple of 5. Thus we can only expect to discover primes among numbers of this form when $n = 4k$, i.e. $2^{4k} + 1$. This news will not startle Number Theory addicts but it is still a fair stride from our initial observation that 'all powers of ten have the terminal digit 0'.

The enquiry started at the beginning of this chapter can, of course be carried much further and indeed the examination of the remainders left after dividing $x^n$ by the successive primes 7, 11, 13, . . ., leads into an extremely interesting and advanced field.

However our two primitive tables (14*a* and 14*b*) can still provide a mass of information about exponential numbers which are multiples of 5 and 3.

It will be seen at once, for example, that $x^n + x^{n+2}$ always has the terminal digit 5 (and hence is a multiple of 5) when $x = 10k +$ 2, 3, 5, 7, 8. Similarly $2^n + 2^{n+1}$ is obviously a multiple of 3 and this can be extended to $x^n + x^{n+1}$ when $x = 9k + 2, 5, 8$.

The more general numbers $x^n \pm y^m$ can also be separated into multiples of these two factors and a few examples are given here which the reader may care to disentangle for himself.

Multiples of 5.

$$2^{4r+1} + 3^{4s+1}$$
$$2^{4r+1} + 7^{4s-1}$$
$$2^{4r-1} + 8^{4s-1}$$

and as an example of still wider generalisation,

$$(10k + 7)^{4r+1} - (10j + 3)^{4s-1}.$$

where $k, j, r, s,$ take any of the values 0, 1, 2, 3, . . ..

Multiples of 3.

$$2^{6r+1} + 5^{6s+2}$$
$$7^{n+1} - 7^n$$

and $(9k + 2)^{6r-1} + (9j + 5)^{6s+2}$.

The use of these tables is not, of course, confined to the addition or subtraction of the powers of only two integers. Thus, for instance, if we consider the horizontal line of digits against $x = 2$, in Table 14*a*, we have,

$$2 + 4 + 8 + 6 + 2 + 4 = 26,$$

and it follows that

$$(2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6) - 1$$

is divisible by five.

In a similar manner Table 14*b* tells us that

$$1^0 + 2^1 + 3^2 + 4^3 + 5^4 + 6^5 + 7^6$$

is a multiple of nine.

The above principles can be applied in a variety of further instances, not all of them trivial, but the point I am hoping to have made is that sometimes the most unexpected findings can emerge from the development of the simplest of elementary observations.

## EXERCISES

1. What is (*a*) the 'unit's' digit, and (*b*) the digital root of $11^{11}$?
2. In the progression $3^0, 3^1, 3^2, 3^3, . . . 3^n$, what are the powers which have the remainder 1 after dividing by 7?
3. Given that the sum $1^3 + 2^3 + 3^3 + 4^3 + x^3$ is a multiple of nine, $x$ ($<10$) can have two values. What are they?

# 11 FINITE ARITHMETIC

(1) In the last chapter we examined a particular class of numbers—the powers of $x$—with special regard to their remainders after dividing by both 9 and 10. Indeed we started from two simple truths which were obvious by definition, namely that (1) the units digit of any integer remains the same whatever multiple of 10 is added to it, and (2) the 'digital root' of any integer is constant for all additions of $9k$.

We dealt there with two special cases of what is clearly a general statement. If we are considering only the units digits of the integers it might be said that 0 is synonymous with 10, 20, 30, etc., or among digital roots 0 is identical with 9. Similarly it would be just as convenient to mark 0 on a clock face instead of 12, since the cycle starts again at this point. Thus the clock will register the same time in twelve hours or, with perhaps some astronomical or horological reservations, in a thousand years, or any numbers of revolutions. Or to give a further example, whenever two values of $n$ differ by an even number then $(-1)^n$ remains identically the same.

This notion of the 'sameness' of numbers which differ only among themselves by some specified multiple was first crystallised and given a formal mathematical symbol by Gauss towards the end of the eighteenth century. Incidentally, he was in his teens at the time.

What Gauss's notation expresses in fact is that if two integers, $a$ and $b$, differ by a multiple of a particular number $m$ then $a$ is said to be congruent to $b$ with respect to the modulus $m$. In this notation we write $a \equiv b \pmod{m}$ instead of the more familiar algebraic $a - b = xm$. Arithmetical congruence then implies equality except for the addition or subtraction of some multiple of $m$. It will immediately be clear that in the arithmetic 'modulo $m$' there are no integers greater than $m - 1$, hence the term 'finite arithmetic'.

Congruences have much in common with ordinary equations

and indeed are manipulated according to exactly the same rules with the one proviso that the same modulus is retained throughout the operations.

Thus, if $a \equiv x \pmod{m}$, then, all to (mod $m$), we have

$$ar = xr$$
$$a + r = x + r$$
$$a^r = x^r \quad \text{etc.}$$

If in addition $\qquad b \equiv y$

then $\qquad ab \equiv xy$

and $\qquad a \pm b \equiv x \pm y$

Although a congruence can always be multiplied throughout by an integer, cancellation of a factor is not permissible unless the factor is relatively prime to the modulus. For instance it is legitimate to reduce the congruence $48 \equiv 18 \pmod{10}$ by a factor of 3 to give $16 \equiv 6 \pmod{10}$, but we cannot divide by the even factor 6 (which is not prime to 10) without arriving at the false result $8 \equiv 3 \pmod{10}$.

(2) The concept of congruence is no mere mathematical toy; it enables us to express many propositions with economy and elegance and particularly to operate with numbers so large that ordinary methods of calculation would be impossible to apply.

As an elementary example of this technique it might be interesting to re-examine the 'extraction' of digital roots. Since any integer $N$ can be written $a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \ldots + 10^na_n$, and $10 \equiv 1 \pmod{9}$—from which it follows that $10^2 \equiv 1$, $10^3 \equiv 1$, $\ldots 10^n \equiv 1$—it is clear that $N \equiv a_0 + a_1 + a_2 + a_3 + \ldots + a_n \pmod{9}$. Hence $N$ is equal to a multiple of 9 plus the sum of its digits and if the latter is divisible by 9 then so is $N$.

Similar reasoning is equally effective in proving the common test for divisibility by eleven.

For the benefit of any newcomers who find the technique unfamiliar perhaps the following examples will help to clarify the primary methods of operation.

(*A*) We have $\qquad 9 \equiv 2 \pmod{7}$,

then $\qquad 9^2 \equiv 2^2 = 4$

and $9^3 \equiv 36 \equiv 1$, and therefore $9^3$ divided by 7 leaves the remainder 1.

(*B*) Since
$$6 \equiv -1 \pmod 7$$
$$6^2 \equiv (-1)^2 = 1$$

and hence
$$6^{2n} \equiv 1 \pmod 7$$

(*C*)
$$8 \equiv 1 \pmod 7$$
$$4 \equiv \tfrac{1}{2}$$
$$2 \equiv \tfrac{1}{4}$$

and since $15 \equiv 1 \pmod 7$, and $36 \equiv 1 \pmod 7$, it follows that

$$5 \equiv 1/3 \pmod 7$$
$$3 \equiv 1/5 \pmod 7$$
$$6 \equiv 1/6 \pmod 7$$

It is clear that this arithmetic, although confined by the modulus, is free to operate with both negative signs and fractions.

As an example of the power of the congruence technique we will now apply it to an actual computation. It is required, let us say, to find the remainder upon dividing $5^{26}$ by 103. Remembering from a previous chapter that any number can be expressed as the sum of single powers of 2, we first note that $5^{26} = 5^2 \times 5^8 \times 5^{16}$.

With this in mind we now proceed as follows:

$$5^2 \equiv 25 \pmod{103}$$
$$5^4 \equiv 625 \equiv 7$$
$$5^8 \equiv 49$$
$$5^{16} \equiv 2401 \equiv 32$$

It is now required to calculate $5^2 \times 5^8 \times 5^{16} \pmod{103}$ and from the above figures we have,

$$5^2 \times 5^8 \equiv 25 \times 49 = 1225 \equiv 92$$
$$92 \times 5^{16} \equiv 92 \times 32 \equiv 2944 \equiv 60.$$

60 then, is the remainder after dividing $5^{26}$ by 103. To reassure those who might doubt so facile a result, here is the actual division done the hard way.

```
103/1490116119384765625
    103
    ---
     460  481   446
     412  412   412
     ---  ---   ---
      481  699   345
      412  618   309
      ---  ---   ---
       691  813   366
       618  721   309
       ---  ---   ---
        736  928   572
        721  927   515
        ---  ---   ---
         151   147  575
         103   103  515
         ---   ---  ---
          481   446  60 = remainder.
                     ==
```

(3) It will be of interest at this point to demonstrate the strength of modulus arithmetic by an example of its application to a principle of far reaching importance in Number Theory. Fermat's theorem states that if $a$ is any integer and $p$ a prime, then $a^p - a$ is divisible by $p$. Or in congruence notation that $a^p \equiv a \pmod p$. Nearly twenty five centuries ago the Chinese knew this to be true in the case of $a = 2$, and until the early nineteenth century the converse, namely that such a factor $p$ is essentially prime, was accepted. Then in 1819 Sarrus discovered that $2^{341} - 2$ is divisible by 341, a composite number $(11 \times 31)$.

The actual computation of the integer $2^{341} - 2$, containing over a hundred digits, and the subsequent tests for divisibility would present a formidable task, but see what light work our modulo arithmetic makes of it.

We have first
$$2^5 \equiv -1 \pmod{11}$$

Then it follows that
$$(2^5)^{2n} \equiv 1$$

and hence
$$(2^5)^{68} = 2^{340} \equiv 1$$

Similarly
$$2^5 \equiv 1 \pmod{31}$$

and
$$2^{340} \equiv 1$$

Thus both 11 and 31 are divisors of $2^{340} - 1$ and hence also of $2^{341} - 2$.

Fermat's theorem is perhaps more usually expressed in the terms, 'if $p$ is a prime and $a$ is not a multiple of $p$ then $a^{p-1} - 1$ is divisible by $p$'. (More refined statements of the theorem will be referred to later.)

That the converse of this is not always true can be seen from a much simpler example than the above. Putting $a = 4$, and $p = 15$, (a composite number) we have $4^{14} - 1 \equiv 0 \pmod{15}$.

Now $\quad 4 \equiv -1 \pmod 5$ and $\quad 4 \equiv 1 \pmod 3$

So $\quad 4^{14} \equiv 1 \quad\quad 4^{14} \equiv 1$

Hence $4^{14} - 1 \equiv 0 \pmod 5$ and $4^{14} - 1 \equiv 0 \pmod 3$. As a check we have $4^{14} - 1 = 268435455$ which is obviously divisible by both 3 and 5.

There are other variants of this famous theorem which lead into much more advanced theory than can be embarked upon here. As examples I will merely comment that the two following statements are true:

$$3^{120} - 1 \equiv 0 \pmod{11^2}$$
$$2^{1092} - 1 \equiv 0 \pmod{1093^2}.$$

(4) Turning now to another development of congruence theory we consider the squares of the natural numbers, $1^2, 2^2, 3^2, \ldots$. Listing the 'digital roots' of these successive squares we have:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $n^2$ | 1 | 4 | 9 | 16 | 25 | 36 | 49 | 64 | 81 | 100 | 121 . . . |
| *D.R.* | 1 | 4 | 9 | 7 | 7 | 9 | 4 | 1 | 9 | 1 | 4 . . . |

The sequence is clearly repetitive and indeed it is easily shown that however far it is continued no other digits than 1, 4, 7, 9, appear, and since in fact digital roots represent the remainders left after dividing by 9 the set might just as well be written 0, 1, 4, 7. These digits are known in congruence language as 'quadratic residues' modulo 9.

It is easily shown that a closed cycle of this sort will occur with any divisor. Let the remainders (residues) on dividing the successive squares by $n$ be $r_1, r_2, r_3, \ldots$. Then if $x$ is any number we have $(n + x)^2 = n^2 + 2nx + x^2 \equiv x^2 \pmod n$ and $r_n + x$ will have the same value as $r_x$ with a periodic recurrence of the terms. Using a similar argument $(n - x)^2 \equiv x^2 \pmod n$ and hence $r_n - x = r_x$. Therefore for the modulus $n$ there are not more than $\frac{1}{2}n$, or if $n$ is odd, $\frac{1}{2}(n - 1)$, residues to the square numbers.

Quadratic residues to any modulus can be calculated quickly without actually writing down the sequence of square numbers. Since $(x + 1)^2 = x^2 + 2x + 1$ it follows that $r_x + 1 \equiv r_x + 2x + 1 \pmod n$ and for example the residues modulo 13 can be derived in either of the following ways:

| $x$ | $x^2$ | $r^n$ | $x$ | | $r_n$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | | 1 |
| 2 | 4 | 4 | 2 | | 4 |
| 3 | 9 | 9 | 3 | | 9 |
| 4 | 16 − 13 | 3 | 4 | $(9 + 2.3 + 1) - 13 =$ | 3 |
| 5 | 25 − 13 | 12 | 5 | $(3 + 2.4 + 1) - 13 =$ | 12 |
| 6 | 36 − 26 | 10 | 6 | $(12 + 2.5 + 1) - 13 =$ | 10 |
| 7 | 49 − 39 | 10 | 7 | $(10 + 2.6 + 1) - 13 =$ | 10 |
| 8 | 64 − 52 | 12 | 8 | $(10 + 2.7 + 1) - 13 =$ | 12 |
| 9 | 81 − 78 | 3 | 9 | $(12 + 2.8 + 1) - 26 =$ | 3 |
| 10 | 100 − 91 | 9 | 10 | $(3 + 2.9 + 1) - 13 =$ | 9 |
| | | etc. | | | etc. |

Integers which are not residues (mod $n$) are known as non-residue and the two classes are connected in the following manner. For any modulus $n$ the product of two or more residues $(r^p, r^q)$ is also a residue. (For if $r^p \equiv x^2$ and $r^q \equiv y^2 \pmod n$ then $r^p r^q = (xy)^2 \pmod n$.) Also the product of two non-residues is again a residue, but the product of a residue and a non-residue is a non-residue.

In the following table (Table 15) quadratic residues of the odd numbers 3, 5, 7, . . . 49, are listed. In order to show the distinction between a prime and composite modulus the table is divided into two sections. (The residues are given in the order of their appearance in the progressive sequence of square numbers.)

**Table 15**

**Quadratic Residues (to $n^2$)**

| $n$ | residues |
|---|---|
| 3 | 1 |
| 5 | 1, 4 |
| 7 | 1, 2, 4 |
| 11 | 1, 4, 9, 5, 3 |
| 13 | 1, 4, 9, 3, 12, 10 |
| 17 | 1, 4, 9, 16, 8, 2, 15, 13 |
| 19 | 1, 4, 9, 16, 6, 17, 11, 7, 3 |
| 23 | 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6 |
| 29 | 1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22 |
| 31 | 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8 |
| 37 | 1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28 |
| 41 | 1, 4, 9, 16, 25, 36, 8, 23, 40, 18, 39, 21, 5, 32, 20, 10, 2, 37, 33, 31 |
| 43 | 1, 4, 9, 16, 25, 36, 6, 21, 38, 14, 35, 15, 40, 24, 10, 41, 31, 23, 17, 13, 11 |
| 47 | 1, 4, 9, 16, 25, 36, 2, 17, 34, 6, 27, 3, 28, 8, 37, 21, 7, 42, 32, 24, 18, 14, 12 |
| 9 | 1, 4, 0, 7 |
| 15 | 1, 4, 9, 1, 10, 6, 4 |
| 21 | 1, 4, 9, 16, 4, 15, 7, 1, 18, 16 |
| 25 | 1, 4, 9, 16, 0, 11, 24, 14, 6, 0, 21, 19 |
| 27 | 1, 4, 9, 16, 25, 9, 22, 10, 0, 19, 13, 9, 7 |
| 33 | 1, 4, 9, 16, 25, 3, 16, 31, 15, 1, 22, 12, 4, 31, 27, 25 |
| 35 | 1, 4, 9, 16, 25, 1, 14, 29, 11, 30, 16, 4, 29, 21, 15, 11, 9 |
| 39 | 1, 4, 9, 16, 25, 36, 10, 25, 3, 22, 4, 27, 13, 1, 30, 22, 16, 12, 10 |
| 45 | 1, 4, 9, 16, 25, 36, 4, 19, 36, 10, 31, 9, 34, 16, 0, 31, 19, 9, 1, 40, 36, 34 |
| 49 | 1, 4, 9, 16, 25, 36, 0, 15, 32, 2, 23, 46, 22, 0, 29, 11, 44, 30, 18, 8, 0, 43, 39, 37 |

It will be seen from the above table that when $n$ is a prime there are exactly $\frac{1}{2}(n-1)$ residues, all of which are different integers. When $n$ is composite the complete cycle still contains $\frac{1}{2}(n-1)$ residues but some of these are repeated one or more times. When $n$ is a square or contains a square factor, 0 of course appears and may be repeated several times in the complete cycle of residues. The number of different integers comprising the quadratic residues to a given modulus $n$, tell us then whether $n$ is prime or composite. At first sight this may not seem a very practical method of establishing the primality of $n$ but in fact it provides a very useful technique for detecting not only whether $n$ is composite, but if so what are its factors.

As a simple example let us take $n = 13 \times 37 = 481$. Since all squares less than 481 are residues of $n$, we have $Q.R.(n) = 1, 4, 9, \ldots 441$ and the sequence can be continued, since $441 = 21^2$, and $(2 \times 21) + 1 = 43$,

$$\begin{aligned}441 + 43 - 481 &= \phantom{0}3 \equiv 22^2 \pmod{481}\\ 3 + 45 &= 48 \equiv 23^2 \text{ etc.}\\ 48 + 47 &= 95\\ 95 + 49 &= 144 \text{ Stop.}\end{aligned}$$

$144 = 12^2$ which has appeared before, and therefore $n$ is composite. Further, since 144 is a residue of the 25th square we now have $25^2 \equiv 12^2 \pmod{481}$ or $25^2 - 12^2 \equiv 0$. That is $(25-12)(25+12) = 13 \times 37$, the factors of 481. This will be dealt with more fully in a later chapter on factorisation methods.

(5) The study of quadratic residues, to which the above is but the briefest of introductions, has produced many theorems of great importance in the realm of Number Theory but it would not be practicable to advance beyond this stage in a book of this sort.

There are however some observations to be made on the residues to higher powers (than squares) which are neither difficult to grasp nor without their peculiar interest. Consider the residues to a given modulus of numbers of the form $x^k$, where $k$ takes the successive values $1, 2, 3, \ldots$.

The powers of $x$ increase fairly rapidly as $k$ increases but as noted before, in finite arithmetic it is not necessary to calculate these out in full to obtain the required residues. Thus the residues (mod 5) to $2^k$, that is to $1, 2, 4, 8, 16, 32, 64, \ldots$, are obtained simply by multiplying each fresh residue as it is found by 2, discarding of course all multiples of the modulus from the product. In the present case we thus arrive at:

$\underline{1}, 2 \times 1 = \underline{2}, 2 \times 2 = \underline{4}, 2 \times 4 = 8$ and
$8 - 5 = \underline{3}, 2 \times 3 - 5 = 1$

The residues (underlined) are then 1, 2, 4, 3, and the cycle starts again. In other words the $k$th power residues of 2 to the modulus 5 are 1, 2, 3, 4. 5 is of course a prime but do not be hasty in assuming from this that the residues modulo $p$ always contain the integers $1, 2, 3, \ldots (p-1)$; those of $2^k$ (mod 7) for instance are 1, 2, and 4, only.

The following tables (16*a*, *b*, *c*) will serve to illustrate some of the properties of the $k$th power residues; they list the residues to the prime modulo $> 4 < 24$ of the integers 2, 3, and 10 with an extension in the case of 16*c*.

**Table 16a**

**Residues to $2^k$**

| $k$ | (mod) 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 3 | 3 | 1 | 8 | 8 | 8 | 8 | 8 |
| 4 | 1 | 2 | 5 | 3 | 16 | 16 | 16 |
| 5 | 2 | 4 | 10 | 6 | 15 | 13 | 9 |
| 6 |  | 1 | 9 | 12 | 13 | 7 | 18 |
| 7 |  |  | 7 | 11 | 9 | 14 | 13 |
| 8 |  |  | 3 | 9 | 1 | 9 | 3 |
| 9 |  |  | 6 | 5 |  | 18 | 6 |
| 10 |  |  | 1 | 10 |  | 17 | 12 |
| 11 |  |  |  | 7 |  | 15 | 1 |
| 12 |  |  |  | 1 |  | 11 |  |
| 13 |  |  |  |  |  | 3 |  |
| 14 |  |  |  |  |  | 6 |  |
| 15 |  |  |  |  |  | 12 |  |
| 16 |  |  |  |  |  | 5 |  |
| 17 |  |  |  |  |  | 10 |  |
| 18 |  |  |  |  |  | 1 |  |

**Table 16b**

**Residues to $3^k$**

| $k$ | (mod) 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 2 | 4 | 2 | 9 | 9 | 9 | 9 | 9 |
| 3 | 2 | 6 | 5 | 1 | 10 | 8 | 4 |
| 4 | 1 | 4 | 4 |  | 13 | 5 | 12 |
| 5 |  | 5 | 1 |  | 5 | 15 | 13 |
| 6 |  | 1 |  |  | 15 | 7 | 16 |
| 7 |  |  |  |  | 11 | 2 | 2 |
| 8 |  |  |  |  | 16 | 6 | 6 |
| 9 |  |  |  |  | 14 | 18 | 18 |
| 10 |  |  |  |  | 8 | 16 | 8 |
| 11 |  |  |  |  | 7 | 10 | 1 |
| 12 |  |  |  |  | 4 | 11 |  |
| 13 |  |  |  |  | 12 | 14 |  |
| 14 |  |  |  |  | 2 | 4 |  |
| 15 |  |  |  |  | 6 | 12 |  |
| 16 |  |  |  |  | 1 | 17 |  |
| 17 |  |  |  |  |  | 13 |  |
| 18 |  |  |  |  |  | 1 |  |

### Table 16c

### Residues to $10^k$

| $k$ | (Mod) 7 | 11 | 13 | 17 | 19 | 23 | 31 | 37 | 41 | 43 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 3 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| 2 | 2 | 1 | 9 | 15 | 5 | 8 | 7 | 26 | 18 | 14 |
| 3 | 6 | | 12 | 14 | 12 | 11 | 8 | 1 | 16 | 11 |
| 4 | 4 | | 3 | 4 | 6 | 18 | 18 | | 37 | 24 |
| 5 | 5 | | 4 | 6 | 3 | 19 | 25 | | 1 | 25 |
| 6 | 1 | | 1 | 9 | 11 | 6 | 2 | | | 35 |
| 7 | | | | 5 | 15 | 14 | 20 | | | 6 |
| 8 | | | | 16 | 17 | 2 | 14 | | | 17 |
| 9 | | | | 7 | 18 | 20 | 16 | | | 41 |
| 10 | | | | 2 | 9 | 16 | 5 | | | 23 |
| 11 | | | | 3 | 14 | 22 | 19 | | | 15 |
| 12 | | | | 13 | 7 | 13 | 4 | | | 21 |
| 13 | | | | 11 | 13 | 15 | 9 | | | 38 |
| 14 | | | | 8 | 16 | 12 | 28 | | | 36 |
| 15 | | | | 12 | 8 | 5 | 1 | | | 16 |
| 16 | | | | 1 | 4 | 4 | | | | 31 |
| 17 | | | | | 2 | 17 | | | | 9 |
| 18 | | | | | 1 | 9 | | | | 4 |
| 19 | | | | | | 21 | | | | 40 |
| 20 | | | | | | 3 | | | | 13 |
| 21 | | | | | | 7 | | | | 1 |
| 22 | | | | | | 1 | | | | |

* The column (mod 29) has been excluded in order to keep the table reasonably compact (it runs to the full length of 28 integers).

The following observations are not intended to replace the proper theoretical approach to this subject—this is competently dealt with in a number of excellent textbooks—but their object is to whet the appetite and to show some examples of how different branches of arithmetic interlock, sometimes in the most unexpected ways.

Probably the first thing that will be noticed in these tables is that whilst there obviously cannot be more than $(n - 1)$ residues to any given modulus $n$, the actual number of residues is in many cases only a fraction of $(n - 1)$. What is more, whenever the $k$th power residues are only $\frac{1}{2}(n - 1)$ in number they are exactly the same values as the quadratic residues to the modulus $n$. (See Table 15.) Looking further into this it will be seen that when there is a full complement of $(n - 1)$ residues to any modulus, those of the even indices, $(k = 0, 2, 4, \ldots)$ are quadratic residues and therefore those of the odd indices are non-residues.

Since in these tables we are dealing with residues to the powers of integers—of the index $k$—this enables us to apply to the multiplication of residues a logarithmic procedure similar to that used in ordinary arithmetic. Thus, to find the product (mod $n$) of two or more residues it is only necessary to add their corresponding $k$ values together and then find the residue in line with this new $k$.

The procedure will be illustrated by taking an example from each table. First, from Table 16*a*, if we take two values in the (mod 13) column, say 8 and 12 the product of which is 96. Then $96 \equiv 5 \pmod{13} \equiv 2^9$. The $k$ values corresponding to 8 and 12 are 3 and 6, which added together equal 9.

Similarly, (Table 16*b*) to the modulus 11:

$$3 \times 9 = 27 \equiv 5 \equiv 3^3, \text{ and } 1 + 2 = 3.$$

Again, (Table 16*c*) to the modulus 19:

$$6 \times 17 = 102 \equiv 7 \equiv 10^{12}, \text{ and } 4 + 8 = 12.$$

(6) It is now possible to provide an explanation for the rule given previously concerning the multiplication of quadratic and non-quadratic residues. The addition of two even or two odd $k$'s produces an even $k$, and hence a quadratic residue, whilst the addition of one even and one odd $k$ is always an odd value and therefore a quadratic non-residue.

Attentive readers will by now, I am sure, have noticed that the sequence of residues (mod 19) to $2^k$ and $10^k$ are identical but in reverse; how many, I wonder, have associated this sequence with that described in earlier chapters (*a*) for determining whether a given number is divisible by 19, and (*b*) as part of one process for constructing the recurring decimal of 1/19.

EXERCISES

1. Show that 101 is a divisor of 99999999.
2. Show that $2^{22} - 1$ is divisible by 23.
3. The following five numbers all have the correct 'endings' and digital roots of square numbers. Given that the quadratic residues of 7 and 11 are respectively (0, 1, 2, 4) and (0, 1, 3, 4, 5, 9) find two of the five which cannot be square.

| | |
|---|---|
| *a* | 2544025 |
| *b* | 2908456 |
| *c* | 2712609 |
| *d* | 2893401 |
| *e* | 2354464 |

# 12 FACTORISATION

(1) A large part of that branch of mathematics somewhat loosely termed 'Number Theory' is either devoted to, or has its origins in the quest for prime numbers. The determination of whether a given (large) number is prime, or if not what are its prime factors, is frequently a matter of interest and more often than not one of considerable difficulty. In this chapter we shall examine some of the methods which have been developed for reducing these difficulties.

Large numbers or small, there are of course some elementary observations which can be made at once. Even numbers and multiples of 5 are recognisable at sight, multiples of 3 respond to a simple and rapid mental check and thanks to a lucky combination of factors those of 7, 11, 13 and 37 are found with little effort.

As we have seen in an earlier chapter many other of the smaller primes can be eliminated without having to use the laborious process of testing by actual division. These methods obviously dispose of vast quantities of the natural numbers—even numbers and multiples of 3 alone take care of two-thirds of them, for instance—but there remains an infinity of integers which are either prime or have larger prime factors than the methods used in chapters 1 and 2 are equipped to deal with. These can be divided broadly into two classes; in the one case numbers of a particular structure such as, say, those expressed generally by the formula $x^n \pm 1$ for which the 'form' of possible factors can usually be determined fairly easily. On the other hand there are amorphous numbers, or shall we say numbers of no known history, whose factor forms can only be found by congruence techniques which for numbers of six or seven digits are inferior to other methods of factorisation and are quite impracticable for larger numbers.* Incidentally, it must be noted that in testing a given number $N$ for possible prime factors it is not necessary to

* See *Advanced Algebra*, Barnard & Child, pp. 192–3.

try a divisor greater than $\sqrt{N}$ since if there is a factor larger than this there must also be a smaller one which has already been disclosed.

Since testing by direct division by the primes in sequence is apparently only really applicable to numbers already well covered by published factor tables it would seem that there is little point in pursuing this method further. As we shall see later, however, in one of the most successful methods of factorisation it is of the utmost importance to determine the highest possible limit of primes which are *not* factors of the number we are trying to crack. Apart from this it will be obvious that if we have eliminated all the primes less than the cube root of a given number $N$ then there can be at most two factors of $N$ and one of these must lie between $\sqrt[3]{N}$ and $\sqrt{N}$, clearly a piece of valuable information.

(2) The best way of testing a number of small prime divisors 'en bloc' is to employ Euclid's Algorithm for finding the H.C.F. (highest common factor) of two numbers. In essence this depends upon the fact that if two numbers have a factor in common then the remainder after dividing one by the other will also contain this factor. Similarly, on dividing this remainder into the previous divisor if there is a further remainder this will also contain the factor, and so on. Continuing in this manner the position is finally arrived at where either the remainder $r_n$ equals 1, in which case both numbers are relatively prime, or $r_{n-1}$ is a multiple of $r_n$. In the latter event the integer $r_n$ is the greatest common factor of the two numbers.

As so often happens in arithmetic the method is far simpler to operate than to describe and an elementary example should clarify the above explanation. Taking the numbers 21 and 56, we proceed to divide thus:

$$56/21 = 2, + 14; 21/14 = 1, + 7; 14/7 = 2 \text{ exactly},$$

and therefore the last divisor—7—is the H.C.F. of the two numbers 21 and 56.

It will be obvious then from the above that if we prepare a composite number containing as factors all the prime divisors we wish to test as possible factors of a given number $N$, Euclid's Algorithm will supply the answer. It is conventional to express the product of successive primes by the Greek capital $\Pi$, and specifically for instance the product of 3 . 7 . 11 . 13 . . . . 101 is written $\underset{3\leqslant p\leqslant 101}{\Pi(p)}$. (For obvious reasons 5 need not usually be included.) The following example will show the basic principles of this method of factorisation.

Let $$N = 943.$$

Now 943 is clearly not a multiple of 3, nor yet of 7, 11, or 13. And since it is less than $31^2$ its only possible factors are then 17, 19, 23, or 29. The product of these four primes is 215441. The algorithm then proceeds;

```
              943)215441
                  1886
                  ----
                   2684
                   1886
                   ----
                    7981
                    7544
                    ----
Remainder =         437)943
                        874
                        ---
Remainder =              69)437
                            414
                            ---
Remainder =                  23)69
                                69
                                --
                                 0
```

And therefore 23 is a factor of 943.

The following illustration is given, not with the intention of boring the reader, who can easily skip it if he feels inclined, but in order to give those interested some feel of the 'weight' of the calculation for numbers of a moderate size. The 'time' advantage over trial divisions by the separate primes increases with the size of $N$.

We shall examine the number $N = 20{,}699{,}411$, and since the primes 3, 7, 11, 13, and 37 can be so readily eliminated it will be assumed that they have been already tested and we then formulate

$$\underset{17\leqslant p\leqslant 53}{\Pi(p)} \quad (\text{ex } 37) = 29330271959743.$$

The algorithm then proceeds:

```
20699411/29330271959743
       20699411
        86308609
        82797644
         35109655
         20699411
         144102449
         124196466
          199059837
          186294699
           127651384
           124196466
            34549183
            20699411
            13849772/20699411
                    13849772
                     6849639/13849772
                           13699278
                              150494/6849639
                                 601976
                                  829879
                                  752470
                                   77409/150494
                                         77409
                                         73085

                       73085/77409
                            73085
                             4324/73085
                                  4324
                                 29843
                                 25944
                                  3901/4324
                                      3901
                                       423/3901
                                          3807
                                           94/423
                                             376
                                              47/94
                                                94
                                                 0
```

Therefore 47 is a factor of $N$.

Dividing out, we have $N = 47 \times 440413$

To continue with the next few possible prime divisors we take

$$59 \,.\, 61 \,.\, 67 \,.\,.\,.\,.\,.\, 83 = \prod_{59 \leqslant p \leqslant 83}(p) = 8472681192817.$$

```
440413/8472681192817
      440413
      4068551
      3963717
       1048341
        880826
        1675159
        1321239
         3539202
         3523304
          1589881
          1321239
           2686427
           2642478
            43949/440413
                 43949
                   923/43949
                       3692
                        7029
                        6461
                        568/923
                            568
                            355/568
                               355
                               213/355
                                  213
                                  142/213
                                     142
                                      71/142
                                        142
                                         0
```

Therefore 71 is a factor of 440413.

Thus $N = 20699411 = 47 \times 71 \times 6203$. Moreover since $\sqrt{6203}$ is less than 80 and all primes up to and including 83 have been tested then 6203 is prime and we have the complete factorisation.

For dealing with large numbers the time consumed by this procedure is relatively trivial and it is generally preferable to employ stages of much larger $\Pi(p)$s.

To save some duplication of effort I give below the products of primes which I have found most convenient in practice.

**Table 17**

**Products of Successive Primes $\Pi(p)$**

| $\Pi(p)$ | |
|---|---|
| $17 \leqslant p \leqslant 89$ (ex 37) | 21391889098600094293679777521 |
| $97 \leqslant p \leqslant 173$ | 7008780881790737660918902153322941 |
| $179 \leqslant p \leqslant 251$ | 385775665012409154140882380977413 |
| $257 \leqslant p \leqslant 337$ | 231050535484280435538943196422625393 |
| $347 \leqslant p \leqslant 419$ | 3236374326887641816997742721494821 |
| $421 \leqslant p \leqslant 499$ | 17861723378516715340736738647007161271 |

There is no need to be intimidated by the size of these numbers; the first division may take a little time but after the first remainder is found the rest of the algorithm requires only a matter of minutes. Generally speaking a number of about ten or twelve digits can be tested for all the prime divisors less than 500 in under the hour and if a hand or desk calculator is available this time will be considerably reduced.

Naturally if we are dealing with a number whose only possible factors are of a particular 'form' it is only necessary to use primes of this form in preparing multiple products for use in the algorithm. This means that either the time involved can be cut or the tests can be carried to much higher values of $p$.

(3) We turn now to a method of factorisation which is infallible, at least in theory. The qualification must be made because there are, of course, random numbers of such magnitude that the labour involved in any computational method is prohibitive.

This method is practicable for numbers of up to about twenty digits, although it must be admitted that if the number turns out to

be prime, as in the case of $I_{19}$, the amount of man-hours required for the test calls for some dedication.

The procedure is based on an identity known to every schoolboy, namely that

$$x^2 - y^2 = (x + y)(x - y), x > y.$$

It is easily shown that all odd numbers can be expressed as the difference of two squares. For if $N$, an odd number, is equal to $ab$, then $a$ and $b$ are both odd and $(a + b)$ and $(a - b)$ are therefore even. Then

$$\left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = \frac{4ab}{4} = ab = N$$

When $N$ is prime then $x + y = N$, and $x - y = 1$, as seen in the example $13 = (7 + 6)(7 - 6) = 7^2 - 6^2$. Composite numbers can also be expressed in this manner but in addition, in at least one other way. Thus when $N = 105$ we have:

$$\begin{aligned} 105 &= 53^2 - 52^2 = (53 + 52)(53 - 52) = 105 \times 1. \\ &= 19^2 - 16^2 = (19 + 16)(19 - 16) = 35 \times 3. \\ &= 13^2 - 8^2 = (13 + 8)(13 - 8) = 21 \times 5. \\ &= 11^2 - 4^2 = (11 + 4)(11 - 4) = 15 \times 7. \end{aligned}$$

In order then to divide a given odd number $N$ into two factors it is necessary to find two squares which have $N$ as their difference. In practice this is effected by subtracting $N$ in turn from a rising sequence of square numbers until a square turns up in the remainders. To take a simple example, let $N = 217$. The first square greater than 217 is $15^2 = 225$, and we might then proceed as follows:

$$\begin{array}{rrrrr} 15^2 = 225 & 16^2 = 256 & 17^2 = 289 & 18^2 = 324 & 19^2 = 361 \\ \underline{217} & \underline{217} & \underline{217} & \underline{217} & \underline{217} \\ 8 & 39 & 72 & 107 & 144 \end{array}$$

Now $144 = 12^2$, and therefore $217 = 19^2 - 12^2 = 31 \times 7$.

This example serves to illustrate the basic principle of the method but the technique is far too clumsy to apply to large numbers. However, a simple manoeuvre enables us to set out the work in a much more compact and workmanlike fashion.

Since $(n + 1)^2 = n^2 + (2n + 1)$, successive squares increase by successive odd number increments and in consequence the differences between the rising squares and $N$ will increase by the same increments. Thus the above individual subtractions can be replaced by cumulative sums in the following manner.

$$\begin{array}{rr}
 & 15^2 = 225 \\
 & N = \underline{217} \\
 & 8 \\
(2 \times 15) + 1 = & \underline{31} \\
16^2 - N = & \overline{39} \\
 & \underline{33} \\
17^2 - N & 72 \\
 & \underline{35} \\
\text{etc.} & 107 \\
 & \underline{37} \\
 & 144 = 12^2
\end{array}$$

(4) The above introduction to this subject will be expanded later, but first it is obviously important to be able to recognise a square when one is found. When dealing with moderately small numbers it is only necessary to have at hand a table of square numbers of which many are available. As $N$ becomes large, however, one must eventually resort to the traditional method of square root extraction. Even so there are some observations to be made which will reduce this necessity to a minimum.

It has already been noted that the digital roots of square numbers—that is, the quadratic residues of 9—can only be 1, 4, 7, and 9 and this is a test which can be applied with speed. Examination of a table of squares will also show that the last two or three digits of square numbers are confined to certain definite patterns. Using the convention that $\underline{0}$ represents any *even* digit and $\underline{1}$, any *odd* digit, it will be seen that the only possible 'square endings' are $\underline{0}1$, $\underline{0}4$, $\underline{1}6$, $\underline{0}9$, 00, and 125, 225, 625. A still closer inspection reveals that a further restriction can put upon numbers with the endings $\underline{0}1$ and $\underline{0}9$, namely that squares in these categories can only have the following forms of endings:

| | |
|---|---|
| . . . $\underline{0}01$ | . . . $\underline{0}09$ |
| . . . $\underline{1}21$ | . . . $\underline{1}29$ |
| . . . $\underline{0}41$ | . . . $\underline{0}49$ |
| . . . $\underline{1}61$ | . . . $\underline{1}69$ |
| . . . $\underline{0}81$ | . . . $\underline{0}89$ |

Numbers satisfying these conditions are still not necessarily square but if the suspect number is large it may be preferable to make further tests by division by small primes rather than resort to the tedious process of root extraction. For instance if on division by 7 the remainder (residue) is not 0, 1, 2, or 4 (see Table 15), the number is not square.

Taken together the above tests will eliminate a considerable number of integers which cannot possibly be squares.

(5) We are now equipped to attempt the factorisation of a moderately large number and I have chosen one of sufficient magnitude to demonstrate both the power of the method and also to leave some elbow room for the development of some useful short-circuiting techniques.

Let, for example, $N = 1{,}002{,}387{,}143$. To begin with the smallest square greater than $N$ is found by the customary square root extraction process, thus:

$$\begin{array}{lrl}
 & 3\ 1\ 6\ 6\ 1^2 & \\
 & 1002387143 & \\
 & \underline{9} & \\
61 & 102 & \\
 & \underline{61} & \\
626 & 4138 & \\
 & \underline{3756} & \\
6326 & 38271 & \\
 & \underline{37956} & \\
63321 & 31543 & \text{(to ensure that the} \\
 & \underline{63321} & \text{square is larger than} \\
 & -\ 31778 & N\text{)}
\end{array}$$

We now have $N = 31661^2 - 31778$ and the successive differences from the rising sequence of squares are found as follows: (Note that $2 \times 31661 + 1 = 63323$)

$$\begin{array}{rl}
31778 & \\
63323 & \\
\hline
95101^{*} & = 31662^2 - N \\
63325 & \\
\hline
158426 & \\
63327 & \\
\hline
221753 & \\
63329 & \\
\hline
285082 & \\
63331 & \\
\hline
348413 & \\
63333 & \\
\hline
411746 & \\
63335 & \\
\hline
475081^{*} & = 31668^2 - N \\
63337 & \\
\hline
538418 & \\
63339 & \\
\hline
601757 & \\
63341 & \\
\hline
665098 & \\
63343 & \\
\hline
728441^{*} & = 31672^2 - N \\
63345 & \\
\hline
791786 & \\
\text{etc.} &
\end{array}$$

It will be seen (the reader can confirm this by continuing the column) that after ten steps the final digits of the sums begin to repeat themselves in the same order, and that in addition the penultimate digits have the same parity as their predecessors. Furthermore we note that in the intervals of ten steps only two sums have the two terminal digits of a possible square*. These correspond with the numbers $31662^2 - N$, and $31668^2 - N$ and are 95101 and 475081 respectively.

Owing to the cyclic pattern of the 'endings' it follows that the only sums in which squares can possibly appear are those related to the squares $31662^2$, $31672^2$, $31682^2$, . . . and $31668^2$, $31678^2$, . . .

etc. We can therefore dispense with the intermediate steps and set up two columns, each of which will advance at ten times the rate we started with.

This presents no difficulties since we are using here an Arithmetical Progression and the total sum of ten such steps is readily found by coupling them in five equal pairs, thus:

$$\begin{array}{rcrcrl}
63325 & & 63327 & & 63329 & \\
63343 & & 63341 & & 63339 & \\
\cline{1-1}\cline{3-3}\cline{5-5}
126668 & & 126668 & & 126668 & \text{etc. and } 5 \times 126668 = 633340.
\end{array}$$

(Note. Each successive 'ten steps' increment increases by 200, and in fact it is easily shown by A.P. formulae that when, as in this case, the common difference per 'step' is 2, then the incremental increase for $n$ steps is $2n^2$. Thus the increase for one step is 2, for 10 steps—200, 20 steps—800, 90 steps—16200, and so on.)

To proceed we now set up the following columns:

$$\begin{array}{rlcrl}
95101 & = 31662^2 - N & & {*}\ 475081 & = 31668^2 - N \\
633340 & & & 633460 & \\
\cline{1-1}\cline{4-4}
{*}\ 728441 & = 31672^2 - N & & 1108541 & = 31678^2 - N \\
633540 & & & 633660 & \\
\cline{1-1}\cline{4-4}
1361981 & \text{etc.} & & {*}1742201 & \text{etc.} \\
633740 & & & 633860 & \\
\cline{1-1}\cline{4-4}
{*}1995721 & & & 2376061 & \\
633940 & & & 634060 & \\
\cline{1-1}\cline{4-4}
2629661 & & & {*}3010121 &
\end{array}$$

None of these sums are squares but we now note that whilst they all have the required last two digits of squares only those starred have the necessary parity for the third digit from the last. Successive A.P. numbers are always rigid pattern-followers and if the above columns are extended it will still be found that only every other sum has the three permissible terminal digits of a possible square.

It is therefore possible to reduce the number of successive additions still further, this time to cover twenty of the original steps. As the following columns will now have all the correct terminal digits of squares we shall pay attention to the digital roots in the next summations. Starting with the starred members of the last columns we then proceed:

| | D.R. | | D.R. |
|---|---|---|---|
| $728441 = 31672^2 - N$ | 8 | $475081 = 31668^2 - N$ | 7 |
| 1267280 | | 1267120 | |
| $1995721 = 31692^2 - N$ | 7 | 1742201 | 8 |
| 1268080 | | 1267920 | |
| 3263801 | 5 | 3010121 | 8 |
| 1268880 | | 1268720 | |
| 4532681 | 2 | $4278841 = 31728^2 - N$ | 7 |
| 1269680 | | 1269520 | |
| $5802361 = 31752^2 - N$ | 7 | 5548361 | 5 |
| | | 1270320 | |
| | | 6818681 | 2 |
| | | 1271120 | |
| | | $8089801 = 31788^2 - N$ | 7 |

Note that as each of the above additions is equivalent to twenty of the original steps the increments increase each time by 800. It will also be seen that the only digital root of a square to appear in this cycle—namely 7—occurs at every third sum (i.e. at every sixty of the original steps). Consequently there is no point in looking for squares in the sums of anything but the $(31692 + 60k)^2 - N$, and $(31668 + 60k)^2 - N$ cycles, and as no squares have yet appeared we now set up two further columns which in addition to having the required terminal digits will contain only sums possessing the digital root of 7. (Incidentally, since each of these sums will now correspond to 60 of the original steps each addition increases by $2 \times 60^2 = 7200$.)

| | |
|---|---|
| $1995721 = 31692^2 - N$ | $4278841 = 31728^2 - N$ |
| 3806640 | 3810960 |
| $5802361 = 31752^2 - N$ | $8089801 = 31788^2 - N$ |
| 3813840 | |
| $9616201 = 31812^2 - N$ | |

We now have a square at last, for $9616201 = 3101^2$.

$$\begin{aligned}\text{Hence } N = 1002387143 &= 31812^2 - 3101^2\\ &= (31812 + 3101)(31812 - 3101)\\ &= 34913 \times 28711.\end{aligned}$$ Which is the complete factorisation.

Shorn of explanatory verbiage and repetitions in the columns the above process can be seen to be remarkably economical in both time and paper: it is still open to further refinement as will be shown later. At the same time modifications of the technique may sometimes be required; with some $N$s, for instance, the (square) digital roots are not evenly spaced and this entails setting up four columns at this stage. There should be no difficulty, however, in extemporising to meet any situation if the above arguments have been thoroughly mastered.

(6) A fundamental difficulty arises in this method of factorisation when $N$ has only two factors which have widely different orders of magnitude. When this happens, or in the extreme case when $N$ is both large and prime, the operation becomes prolonged, perhaps to an intolerable extent.

If the process then is to remain practicable in such circumstances it is essential to find some way of at least reducing this difficulty.

Now it will be clear that however many factors $N$ may possess the method described above produces only two; one or both of these may of course be composite.

Let $N = ab$, and as we want $N$ in the form $x^2 - y^2$ then we must have $a = x + y$, and $b = x - y$.

(It should be noted that since $N$ is odd—or can be made so by division by some power of 2—then both $x + y$ and $x - y$ must also be odd.)

If $a$ and $b$ are of the same order of magnitude we can say that $a \sim b \sim \surd N$, which implies that $y$ is relatively small and will be found early in the proceedings. On the other hand if $a$ and $b$ differ appreciably then it can be said that $a =$ (approximately) $kb$, where $k$ is an integer. Obviously if $k$ can be found then $kN$ will have the two nearly equal factors $a$ and $kb$ which will quickly be disclosed.

Unfortunately there is no way of predicting the value of $k$ and so it can only be found by trial. That is, if the above algorithm shows no signs of finding a square it should be abandoned and a new test started on $3N$, then on $5N$, and so on. (The reason why even values of $k$ are not recommended can be explained as follows. When $k$ is odd then both $x + y$ and $x - y$ must be odd and the condition noted above is satisfied. When, however $a$ is nearly equal say to $2b$ and the algorithm is applied to $2N$ no solution will emerge because we have now made one of the factors even whilst the other remains odd and it is no longer possible for them to assume the forms $x + y$ and $x - y$. Furthermore, if $4N$ is tried, although now both new factors will be even they will be in the same ratio as before and no advantage will have been gained. In such a case, therefore, $N$ must be multiplied by 8 before the new factors become nearly equal, and in general if $k$ is an even number $N$ must be multiplied by $4k$.)

To recapitulate, it has been shown that if $N = ab$ and $a \sim kb$, then the difference of squares method will quickly produce the factors of $N$ if it is applied to

$kN$ when $k$ is an odd number,
$4kN$ when $k$ is an even number.

It may come as a surprise that increasing the size of the number to be tested actually leads to a quicker solution of the problem but the reader can easily satisfy himself of the truth of this.

It will now be seen why it is important to eliminate as many of the smaller prime divisors as possible before beginning this procedure since we are then able to define the lowest limit of $k$. Thus when it is clear that there are no factors less than, say $W$, the first $k$ to be tried should be just greater than $N/W^2$.

(7) The foregoing process is powerful and yet requires little more than an attention to detail which one must accept in this brand of mathematics. After a few practice shots at numbers of say, three to six digits—Premium Bond numbers provide excellent material—the reader should be able to tackle quite large numbers with confidence. In fact he will be equipped to perform what some writers have regarded as near-miracles.

On the subject of primes, and referring to an often quoted Fermat legend (repeated even as recently as March 1964 in *Scientific American* in almost identical terms), Kasner and Newman in their stimulating book *Mathematics and the Imagination* have this to say (p. 187):

> 'Curiously enough there is reason to believe that certain mathematicians of the seventeenth century, who spent a great deal of time on number theory, had means of recognising primes unknown to us, . . . it is still a source of wonder that Fermat replied without a moments hesitation to a letter which asked whether 100895598169 was a prime, that it was the product of 898423 and 112303, and that each of these numbers was prime. Without a general formula for all primes, a mathematician, even today, might spend years hunting for the correct answer.'

The 'difference of squares' method, which was of course well known to Fermat, breaks this number down almost before we can get started, but look what happens when we apply the process to $8N$. I give the calculation in full in order to show that the time involved is trivial.

We have $N = 1008955981169$; $8N = 807164785352$. Then extracting the square root of $8N$:

```
            807164785352(898424
            64
169         1671
            1521
1788         15064
             14304
17964          76078
               71856
179682          422253
                359364
1796844          6288952
                 7187376
               -  898424
```

Thus

$$\begin{aligned} 8N &= 898424^2 - 898424 \\ &= 898424\,(898424 - 1) \\ &= 8 \times 112303 \times 898423 \end{aligned}$$

Therefore $N = 112303 \times 898423$.

So much for 'lost methods', 'general formulae for primes' and 'years of hunting'.

(8) Before ending this chapter it will perhaps be appropriate to include a note on 'checking the work'. In calculations of this kind, which may on occasion become protracted, it is always well at intervals to check the accuracy and the progress of the operation.

This is easily carried out and it will be enough to give only a simple example.

Suppose the 'difference of squares' algorithm is being applied to $N = 3527$, a number which is easily seen to have none of the factors 3, 7, 11, and 13. The working starts with

$$N = 60^2 - 73$$

and proceeds to the point

$$N = 126^2 - 12349$$

without a square number appearing. At this stage it is decided to make a check.

The largest square less than 12349 is $111^2 = 12321$ which differs from 12349 by 28.

Now:

$$126^2 - 111^2 = 15 \times 237 = 3555,$$

And

$$3555 - N = 28.$$

Therefore the calculations are without error and furthermore the check shows that all the primes between $\sqrt{N}$ and 15 have been tested. It follows that 3527 must therefore be prime.

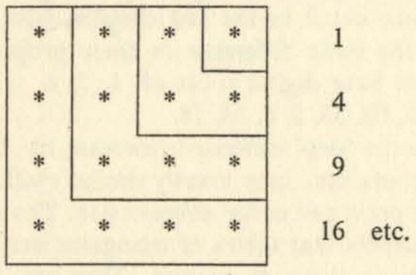
This method of checking should never be neglected since it not only confirms the accuracy of the work but at the same time provides an indication of when one should start again with a new value of $kN$.

### EXERCISES

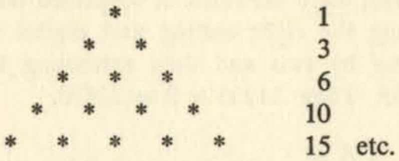
1. Find one factor common to both 16733 and 35699.
2. $N = 1181027$ has one factor less than 30. What is it?
3. Using the 'difference of squares' method find the factors of $N = 1093709$.

# 13 MORE FACTORISATION METHODS

(1) We are all familiar with the 'square' numbers, which can be represented graphically in the form:



'Triangular' numbers are those formed by the cumulative sums of the rows in a triangular array, thus:



and they produce a sequence of which the $n$th term is

$$\frac{n(n+1)}{2}.$$

These numbers share with the squares many useful properties, not all of which seem to have received full recognition.

In my opinion their employment in factorisation techniques is vastly to be preferred to that of the square numbers. It is easily seen that, just as with the squares, any integer which can be expressed as the difference of two triangular numbers is composite and, when so resolved, the factors can be found immediately.

Thus, $(x > y)$:

$$\frac{x(x+1)}{2} - \frac{y(y+1)}{2} = \frac{x^2 - y^2 + x - y}{2}$$

$$= \frac{(x-y)(x+y) + (x-y)}{2}$$

$$= \frac{(x-y)(x+y+1)}{2}$$

When using these numbers for factorisation the same use can be made of digital roots, terminal digits and multiples of $N$ as those described in some detail in the last chapter, with, of course due recognition of the basic difference in these properties. Thus, triangular numbers have digital roots of 1, 3, 6, and 9, and can only end in 0, 1, 03, 53, 5, 6, 28, 78.

In this system the 'step' increments increase by 1, instead of 2, but the digital roots, etc., have exactly similar cyclic properties and offer the same opportunities for abbreviation. The method has one disadvantage, namely that tables of triangular numbers are not so readily available as those of squares. They are, however, easily constructed particularly if one has access to a hand or desk calculating device, and in any case the loss is not all that important when dealing with large numbers. A suspected triangular number, that is one having the right ending and digital root, is tested by first multiplying by two and then extracting the square root. Thus: $T = 11935$. Then $11935 \times 2 = 23870$.

$$\begin{array}{rll}
 & 1\;5\;4^2 & \\
2T = & 23870 = 154^2 + 154 = 154 \times 155 & \\
 & \underline{1} & \text{and therefore } T = (154 \times 155)/2 \\
25 & 138 & \text{which is of triangular form} \\
 & \underline{125} & \\
304 & 1370 & \\
 & \underline{1216} & \\
 & 154 &
\end{array}$$

After what has been said there should now be no difficulty in understanding the working of the following example.

To find the factors of $N = 437891$ $(= 397 \times 1103)$.

First find the least triangular number $>N$ by extracting the square root of $2N$.

$$\begin{array}{rl}
 & 9\;3\;6^2 \\
2N = & 875782 \\
 & \underline{81} \\
183 & 657 \\
 & \underline{549} \\
1866 & 10882 \\
 & 11196
\end{array}$$

and we have $\dfrac{936 \times 937}{2} = 438516$. (= say, $936_t$)

The calculation then continues:

$$\begin{array}{rrl}
 & 438516 & \\
-N & 437891 & \\
\cline{2-2}
 & 625 & = 936_t - N \\
 & 937 & \\
\cline{2-2}
 & 1562 & \\
 & 938 & \\
\cline{2-2}
 & 2500 & \\
 & 939 & \\
\cline{2-2}
 & 3439 & \\
 & 940 & \\
\cline{2-2}
 & 4379 & (940_t - N) \\
 & 941 & \\
\cline{2-2}
 & 5320 & \\
 & 942 & \\
\cline{2-2}
 & 6262 & \\
 & 943 & \\
\cline{2-2}
 & 7205 & \\
 & 944 & \\
\cline{2-2}
 & 8149 & \\
 & 945 & \\
\cline{2-2}
 & 9094 & \\
 & 946 & \\
\cline{2-2}
 & 10040 & \\
 & 947 & \\
\cline{2-2}
 & 10987 & \\
 & 948 & \\
\cline{2-2}
 & 11935 & = (948_t - N) = 154_t
\end{array}$$

We now have, $N = 948_t - 154_t$ and therefore $N$ is composite, its factors being found as follows:

$$\begin{array}{rr}
 & 948 \\
+ & 155 \\
\hline
 & \underline{\underline{1103}}
\end{array}
\qquad
\begin{array}{rr}
 & 948 \\
- & 154 \\
\hline
 & 794 = 2 \times \underline{\underline{397}}
\end{array}$$

It will be noticed that as each value of $(x_t - N)$ is found $x$ is numerically equal to the previous incremental addition; because of this it is simpler to keep track of the operation than in the difference of squares method. The greatest advantage that the triangular numbers have over the squares in this system of factorisation lies in the number of steps required for ultimate solution. In the above example the factors were found after only twelve steps whereas the 'difference of squares' process requires 87 steps for the same $N$.

(2) We turn now to some less orthodox systems which can be used for finding factors. They are included more for their individual interest than for their practical value in attacking large numbers, although any of them might well repay some development work.

The first is simply a variant on the method described in the last chapter. It is deliberately being treated separately because unlike the former method its power is seen to the best advantage when $N$ is either prime or has factors of widely different orders of magnitude—that is, when $k$ proves to be large.

The principle becomes clear when it is remembered that whilst there are exactly $p - 1$ quadratic residues, all of them different, to any prime $p$, the number of residues to a composite number $M$ is always less than $M - 1$ and some of them are repeated at least once.

Briefly, the process starts with a progression of steps produced in exactly the same way as in the 'difference of squares' method, but in this case the progressive totals are not allowed to exceed $N$ in value. When this occurs $N$ is subtracted and the steps are then continued in the normal way. From this point onward a watch is then kept for any sum which has appeared before and as soon as a duplication is seen the factorisation can be completed.

To give an example of the process, we have:

$$N = 2533 = 51^2 - 68. \qquad (= 17 \times 149. \;\; k \sim 9)$$

Then,

| | | |
|---|---|---|
| 68 | 1311 | 118 |
| 103 | 125 | 145 |
| 171 | 1436 | 263 |
| 105 | 127 | 147 |
| 276 | 1563 | 410 |
| 107 | 129 | 149 |
| 383 | 1692 $(65^2)$ | 559 $(75^2)$ |
| 109 | 131 | 151 |
| 492 $(55^2)$ | 1823 $(66^2)$* | 710 |
| 111 | 133 | 153 |
| 603 | 1956 | 863 |
| 113 | 135 | 155 |
| 716 | 2091 | 1018 |
| 115 | 137 | 157 |
| 831 | 2228 | 1175 |
| 117 | 139 | 159 |
| 948 | 2367 | 1334 $(80^2)$ |
| 119 | 141 | 161 |
| 1067 $(60^2)$ | 2508 | 1495 |
| 121 | 143 | 163 |
| 1188 | 2651 $> N$ | 1658 |
| 123 | 2533 | 165 |
| 1311 | 118 | 1823 $(83^2)$* |

* The sum 1823 has been repeated and the factors are found thus:

$$N = 66^2 - 1823$$
$$2N = 83^2 - 1823$$

Subtracting $N = 83^2 - 66^2 = (83 + 66)(83 - 66)$

And then $N = 149 \times 17.$

As a suggestion for further research into this subject, it might be of interest to note that the residues to triangular numbers have similar properties to quadratic residues and are also duplicated, sometimes at frequent intervals, when $N$ is composite.

(3) The following algorithm is not so much a method of factorisation as a device for reducing the size of the number under test.

I have not seen it mentioned before but that, of course, does not give it any claim to originality.

To find the factors of $N$ first set up a column ($A$) in which the first term is $(N - 1)/2$, the following lines being successively reduced by unity. At the same time odd integers 1, 3, 5, 7, . . . are set alongside these terms in a column ($B$). Then those numbers in col. $B$ which divide their companions in col. $A$ are also divisors of $N$.

To illustrate, we take $N = 1001$. Then $(N - 1)/2 = 500$.

Then proceed,

| *A* | *B* |
|---|---|
| 500 | 1 |
| 499 | 3 |
| 498 | 5 |
| 497 | 7 |

And since $497/7 = 71$, then 7 is a factor of 1001. Furthermore as $(2 \times 71) + 1 = 143 = 11 \times 13$, we have the other factors. Or alternatively the columns could be continued thus:

| | |
|---|---|
| 496 | 9 |
| 495 | 11 $(495 = 11 \times 45)$ |
| 494 | 13 $(494 = 13 \times 38)$ |

Since the integers in col. $A$ decrease by exactly half the increase of those in col. $B$ it is a simple matter to arrange for composite numbers to be omitted from col. $B$, or to skip as many numbers as we like. In the first instance column $B$ can, and indeed should, contain only the odd primes, and in the second whenever the possible factors of $N$ are known to be of a particular 'form' only primes of this form need be tabulated.

Thus, for example if $N = 11111$, and it is known, as we saw earlier, that only numbers of the form $30n + 1$ and $30n + 11$ are eligible then we can proceed as follows:

$$(N - 1)/2 = 5555.$$

Then we have

| | |
|---|---|
| 5555 | 1 |
| 5550 | 11 |
| 5540 | 31 |
| 5535 | 41 |

On testing it is found that $5535/41 = 135$.

And since $(135 \times 2) + 1 = 271$, we have the factors 41 and 271.

This method has the following advantages: it allows little opportunity for errors in calculation; with the aid of factor tables it is effective in quickly eliminating quantities of small primes particularly when they are of known 'form'; and as it starts with $N/2$ it therefore virtually doubles the range of the available factor tables.

(4) The method of factorisation about to be described is taken from L. E. Dickson's *History of the Theory of Numbers* Vol. 1 and therein is attributed to D. Biddle (1911).

It is included here not for its practicability but to provide a basis for speculation on the devious processes which led up to its conception.

*Process.* Express $N$ as $S^2 + A$ where $S^2$ is the largest square $<N$. Write three rows of numbers, the first beginning with $A$, (or $A - S$ if $A > S$); the second beginning with $S$ (or $S + 1$, in the latter case), and increasing by 1, the third beginning with $S$ and decreasing by 1.

Let $A_n$, $B_n$, $C_n$ be the $n$th elements in the respective rows. Then $C_n = C_{n-1} - 1$; $B_n = B_{n-1} + 1$; $A_n = A_{n-1} + B_{n-1} - kC_n$. When $(A_{n-1} + B_{n-1})$ is greater than $C_n$, a multiple of $C_n$ is subtracted so as to leave a positive remainder and then $B_n = B_{n-1} + k$. When a value of $n$ is reached for which $A_n = 0$, then $N = B_n \times C_n$.

For an example we take $N = 589 = 24^2 + 13$

| | | | | | | |
|---|---|---|---|---|---|---|
| $A$ | 13 | 14 | 17 | 1 | 9 | 0 |
| $B$ | 24 | 25 | 26 | 28 | 29 | 31 |
| $C$ | 24 | 23 | 22 | 21 | 20 | 19 |

The factors of $N = 589$ are thus disclosed as 19 and 31.

I am sorry if the above account lacks a certain amount of elegance but am comforted by Dickson's laconic note 'It may be best to start with $2N$.'

EXERCISES

1. Find the divisors of the following numbers using *any* method of factorisation.

| | |
|---|---|
| *a* | 15871 |
| *b* | 15853 |
| *c* | 15863 |

2. The factors of $N = 13333$ are of the form $22k + 1$. What are they?

3. The factors of $N = 548497$ are of the form $26k + 1$. What are they?

# 14 A NOTE ON THE CONVERSE OF FERMAT'S THEOREM

(1) Many readers must have been puzzled on reading that such and such a (large) number is composite but its factors are not known. One would think that the authors of books in which such statements appear—and there are quite a few of them in the 'popular' mathematics field—might have spared a few lines to explain the basic principle on which an observation of this sort depends.

Let us consider Fermat's theorem again. This states in effect, that if $p$ is a prime and $a$ is neither equal to, nor a multiple of $p$, then $(a^{p-1} - 1)$ is a multiple of $p$. Or in congruence language $a^{p-1} \equiv 1 \pmod{p}$. All this is perfectly true but one must be careful not to infer that the converse is necessarily true, namely that if $a^{N-1} \equiv 1 \pmod{N}$ then $N$ must be prime. The probability that it is, is very high but in spite of this it can be proved that there are an infinity of composite $N$'s which satisfy the congruence.

Lucas first laid down, and in 1891 proved the necessary conditions for a true converse of the theorem, namely that 'If $a^x \equiv 1 \pmod{N}$ for $x = N - 1$, but *not* for $x$ a proper divisor of $N - 1$, then $N$ is a prime.'

Since then Lehmer in particular has developed many refinements to the theory, so much so that it can be considered now as one of the few valid tests for the primality of large numbers. The arguments are somewhat advanced and quite beyond the scope of this book; probably the best presentation is to be found in D. H. Lehmer's paper, 'Tests for primality by the converse of Fermat's theorem', *Bull. Amer. Math. Soc.*, vol. 33, 1927, pp. 327–340.

On the other hand the converse presents no difficulties when applied as a test for *composite* numbers, and it is legitimate to conclude that if $a^{N-1} \equiv r \pmod{N}$, where $r$ proves to have any other value than 1, then $N$ is *not* prime and is therefore a product of two or more primes.

To carry out this test is is necessary to find the remainder on

dividing $a^{N-1}$ by $N$ and as $a$ can take any value prime to $N$ it is convenient to let $a = 2$. The actual calculation uses the following properties of a congruence, namely that if $2 \equiv R \pmod{N}$ then $2^2 \equiv R^2, 2^3 \equiv 2R^2$, etc. It is advisable to set out the operations in an orderly manner and the following explanation and the three worked examples—although applied to only small $N$'s—will indicate the procedure to be followed in testing numbers of any magnitude. The calculation employs two columns of figures labelled here $A$ and $2^A \pmod{N}$ respectively. The left hand column ($A$) is constructed first and starts with $N - 1$. Each successive line is obtained by dividing the previous one by 2, (after subtracting 1 if the number is odd). The last entry is, of course 1 and against this the next column is started from the bottom with the number 2. (It is as well at this stage to make a mark against the odd numbers in Col. $A$ as a reminder in what follows.)

The rising sequence of this second column is now formed by successive squaring, the resultant squares also being doubled where the corresponding entries in Col. $A$ are odd. Each value is then divided by $N$ and the remainder entered in the next line above. The final entry at the top of the column is then the residue (mod $N$) of $2^{N-1}$ and if this is any number other than 1 then $N$ is composite.

*Example* 1

$N = 437$

| $A$ | $2^A \pmod{N}$ | |
|---|---|---|
| 436 | 359 | |
| 218 | 213 | |
| 109* | 173 | |
| 54 | 58 | etc. |
| 27* | 170 | $2 \times 111^2 = 24642 \equiv 170 \pmod{437}$ |
| 13* | −111 | $2 \times 64^2 = 8192 \equiv 326 \pmod{437}$ see below |
| 6 | 64 | $8^2$ |
| 3* | 8 | $2 \times 2^2$ |
| 1* | 2 | |

Therefore $2^{437-1} \equiv 359 \pmod{437}$ and $N$ is composite. It should be noted that it is sometimes more convenient to use a negative value as the remainder since this still becomes positive again after squaring. Thus $2 \times 64^2 = 8192 \equiv 326 \pmod{437}$ and $326 - 437 = -111$. It is simpler to square $-111$ than 326, a saving of time which can be significant when the modulus is large.

*Example* 2

$N = 347$

| $A$ | $2^A \pmod{N}$ |
|---|---|
| 346 | 1 |
| 173* | −1 |
| 86 | 120 |
| 43* | 193 |
| 21* | 231 |
| 10 | −17 |
| 5* | 32 |
| 2 | 4 |
| 1 | 2 |

Therefore 347 *may* be prime. (In fact it is.)

*Example* 3

$N = 561$

| $A$ | $2^A \pmod{N}$ |
|---|---|
| 560 | 1 |
| 280 | 1 |
| 140 | 67 |
| 70 | 166 |
| 35* | 263 |
| 17* | —202 |
| 8 | 256 |
| 4 | 16 |
| 2 | 4 |
| 1 | 2 |

Although it is seen that $2^{560} \equiv 1 \pmod{561}$, 561 is *not* prime. It is in fact equal to $3 \times 11 \times 17$.

There is, of course, no need to confine the value of $a$ to 2, though for obvious reasons it is best to keep to small values. If, for any reason one chooses to use $a = 3$, then the base of the right hand column is started with 3, otherwise the procedure follows exactly the same pattern as with $a = 2$.

Again, there is no need, as can be seen in the above examples, to continue the col. $A$ downwards beyond the point where $a^A$ becomes less than $N$ provided suitable power tables are available. (See Appendix.)

# 15 CONCLUSION

(1) In what has gone before I have introduced to the reader a very small section of that branch of mathematics known as the Theory of Numbers. The main theme of the book has been factorisation, a subject which, once the bug has bitten is intensely fascinating and yet at the same time embedded in difficulties. I have hoped to give some indication of how some of these difficulties may be chipped away and to have stimulated an interest in research into the subject.

Let no one be deterred from this by the advent of modern electronic computers and their spectacular success in finding ever larger primes of a particular 'form'; the computer may take only minutes to provide the answer to a given problem but its actual programming may well have required hundreds or even thousands of skilled man-hours to prepare. Nor should we forget that most of these programmes depend for their success upon principles laboriously hammered out and tested by mathematical enthusiasts throughout the ages.

A chapter on some of the known properties of primes was almost essential in this context. They have worried mathematicians, particularly amateurs who presumably have more time to spend on matters of doubtful outcome, since their 'separateness' was first recognised. It may be that the modification to Euler's criterion suggested in this chapter (perhaps with further necessary restrictions), could lead somewhere, in which case it ought not to be unduly difficult to extend the test to numbers of the other forms. On the other hand we may be asking altogether the wrong kind of questions about primes. Perhaps an intensive study of the more general 'relative primes' might in the long run be more profitable. Here indeed there could be scope for a new Einstein.

(2) Of course mathematicians, even Number Theory addicts, do not confine their attentions all the time to such fundamental problems

and it might be fitting to close with a few samples of the many curious observations that have been made from time to time.

1. A property of 24; This is the largest value of $n$ that is divisible by all the integers less than $\sqrt{n}$.

2. A property of 30; When $n = 2, 3, 4, 6, 8, 12, 18, 24, 30$, the integers less than, and relatively prime to $n$ are all unity and primes. No number greater than 30 has this property. (Uspensky & Haslet.)

3. In the following subtractions all the original digits are repeated in the answers once only.

$$\begin{aligned} 9876543210 - 0123456789 &= 9753086421 \\ 987654321 - 123456789 &= 864197532 \\ 98754210 - 01245789 &= 97508421 \end{aligned}$$

4. $54 + 72 + 90 = 6^3$

$$54^3 + 72^3 + 90^3 = 108^3 = (72 + 90 - 54)^3$$

5. All the integers except the powers of 2 can be expressed as the sum of consecutive numbers.

6. The addition of unity to the product of any four consecutive numbers produces a square number.

7. In the number 312132 we have, 1 digit between the 1s,
2 digits between the 2s,
3 digits between the 3s.

Can this system be extended?

8. Some examples of multiplications in which all the digits are used once only:

$$7 \times 9403 = 65821: \quad 3 \times 1458 = 6 \times 729.$$

9. 'Fermat's Quotient', $(2^{p-1} - 1)/p$ is only a square when

$$p = 3 \text{ or } 7.$$

10. $512 = (5 + 1 + 2)^3$:

$$47045881000000 = (47 + 4 + 58 + 81)^6.$$

11. $3^3 + 4^3 + 5^3 = 6^3$
$1^3 + 3^3 + 4^3 + 5^3 + 8^3 = 9^3$
$3^3 + 4^3 + 5^3 + 8^3 + 10^3 = 12^3$
$1^3 + 5^3 + 6^3 + 7^3 + 8^3 + 10^3 = 13^3$
$2^3 + 3^3 + 5^3 + 7^3 + 8^3 + 9^3 + 10^3 = 14^3$

12. $11^3 + 12^3 + 13^3 + 14^3 = 20^3$
$6^3 + 7^3 + 8^3 + \ldots + 68^3 + 69^3 = 180^3$
$1134^3 + 1135^3 + 1136^3 + \ldots + 2132^3 + 2133^3 = 16830^3$

13. $4^5 + 5^5 + 6^5 + 7^5 + 9^5 + 11^5 = 12^5$
$5^5 + 10^5 + 11^5 + 16^5 + 19^5 + 29^5 = 30^5$

14. $4! = 24$
$5! = 120$
$7! = 5040$ All become squares on adding 1.
No similar cases are known below 1020!.

15. $6! \times 7! = 10!$

16. The two numbers 57321 and 60984 together contain the ten digits. Each of the squares of these numbers; 3285697041 and 3719048256 contain all ten digits.

17. (*a*) $1 + 2 = 3$
$4 + 5 + 6 = 7 + 8$
$9 + 10 + 11 + 12 = 13 + 14 + 15$ etc.

The highest L.H. number $= n(n + 1)$

(*b*) $3^2 + 4^2 = 5^2$
$10^2 + 11^2 + 12^2 = 13^2 + 14^2$
$21^2 + 22^2 + 23^2 + 24^2 = 25^2 + 26^2 + 27^2$ etc.

The highest L.H. number $= (2n(n + 1))^2$
But we cannot continue on these lines for

$$5^3 + 6^3 = 7^3 - 2.$$

18. Factors of $10^n$ containing no 0's. Are any to be found between

$10^2 = 4 \times 25$
$10^3 = 8 \times 125$ and
$10^{33} = 8589934592 \times 116415321826934814453125$?

19. Can the following sequence be continued, 1, 3, 8, 120, . . .? (Where the product of any two integers is $x^2 - 1$.)

# APPENDIX

### Square Roots

(To seventeen significant figures)

| $n$ | $\sqrt{n}$ |
|---|---|
| 2 | 1·4142135623730955 |
| 3 | 1·7320508075688773 |
| 5 | 2·2360679774981797 |
| 6 | 2·4494897427831781 |
| 7 | 2·6457513110645906 |
| 8 | 2·8284271247461909 |
| 10 | 3·1622776601683793 |
| 11 | 3·3166247903553998 |
| 13 | 3·6055512754639893 |
| 14 | 3·7416573867739414 |
| 15 | 3·8729833460437668 |
| 17 | 4·1231056256176484 |
| 19 | 4·3657754179526917 |
| 21 | 4·5825756931198854 |
| 22 | 4·6904157598233230 |
| 23 | 4·7958315233127196 |
| 26 | 5·0990195135927848 |
| 29 | 5·3851648071345040 |

### Factorial '*n*'

$$1 \times 2 \times 3 \times 4 \times \ldots \times n = n!$$

| *n* | *n*! |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 6 |
| 4 | 24 |
| 5 | 120 |
| 6 | 720 |
| 7 | 5040 |
| 8 | 40320 |
| 9 | 362880 |
| 10 | 3628800 |
| 11 | 39916800 |
| 12 | 479001600 |
| 13 | 6227020800 |
| 14 | 87178291200 |
| 15 | 1307674368000 |
| 16 | 20922789888000 |
| 17 | 355687428096000 |
| 18 | 6402373705728000 |
| 19 | 121645100408832000 |
| 20 | 2432902008176640000 |
| 21 | 51090942171709440000 |
| 22 | 1124000727777607680000 |
| 23 | 25852016738884976640000 |
| 24 | 620448401733239439360000 |
| 25 | 15511210043330985984000000 |
| 26 | 403291461126605635584000000 |
| 27 | 10888869450418352160768000000 |
| 28 | 304888344611713860501504000000 |
| 29 | 8841761993739701954543616000000 |
| 30 | 265252859812191058636308480000000 |
| 31 | 8222838654177922817725562880000000 |
| 32 | 263130836933693530167218012160000000 |
| 33 | 8683317618811886495518194401280000000 |
| 34 | 295232799039604140847618609643520000000 |

### Triangular Numbers $n(n + 1)/2$

| *n* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 3 | 6 | 10 | 15 | 21 | 28 | 36 | 45 |
| 1 | 55 | 66 | 78 | 91 | 105 | 120 | 136 | 153 | 171 | 190 |
| 2 | 210 | 231 | 253 | 276 | 300 | 325 | 351 | 378 | 406 | 435 |
| 3 | 465 | 496 | 528 | 561 | 595 | 630 | 666 | 703 | 741 | 780 |
| 4 | 820 | 861 | 903 | 946 | 990 | 1035 | 1081 | 1128 | 1176 | 1225 |
| 5 | 1275 | 1326 | 1378 | 1431 | 1485 | 1540 | 1596 | 1653 | 1711 | 1770 |
| 6 | 1830 | 1891 | 1953 | 2016 | 2080 | 2145 | 2211 | 2278 | 2346 | 2415 |
| 7 | 2485 | 2556 | 2628 | 2701 | 2775 | 2850 | 2926 | 3003 | 3081 | 3160 |
| 8 | 3240 | 3321 | 3403 | 3486 | 3570 | 3655 | 3741 | 3828 | 3916 | 4005 |
| 9 | 4095 | 4186 | 4278 | 4371 | 4465 | 4560 | 4656 | 4753 | 4851 | 4950 |
| 10 | 5050 | 5151 | 5253 | 5356 | 5460 | 5565 | 5671 | 5778 | 5886 | 5995 |
| 11 | 6105 | 6216 | 6328 | 6441 | 6555 | 6670 | 6786 | 6903 | 7021 | 7140 |
| 12 | 7260 | 7381 | 7503 | 7626 | 7750 | 7875 | 8001 | 8128 | 8256 | 8385 |
| 13 | 8515 | 8646 | 8778 | 8911 | 9045 | 9180 | 9316 | 9453 | 9591 | 9730 |
| 14 | 9870 | 10011 | 10153 | 10296 | 10440 | 10585 | 10731 | 10878 | 11026 | 11175 |
| 15 | 11325 | 11476 | 11628 | 11781 | 11935 | 12090 | 12246 | 12403 | 12561 | 12720 |
| 16 | 12880 | 13041 | 13203 | 13366 | 13530 | 13695 | 13861 | 14028 | 14196 | 14365 |
| 17 | 14535 | 14706 | 14878 | 15051 | 15225 | 15400 | 15576 | 15753 | 15931 | 16110 |
| 18 | 16290 | 16471 | 16653 | 16836 | 17020 | 17205 | 17391 | 17578 | 17766 | 17955 |
| 19 | 18145 | 18336 | 18528 | 18721 | 18915 | 19110 | 19306 | 19503 | 19701 | 19900 |
| 20 | 20100 | 20301 | 20503 | 20706 | 20910 | 21115 | 21321 | 21528 | 21736 | 21945 |
| 21 | 22155 | 22366 | 22578 | 22791 | 23005 | 23220 | 23436 | 23653 | 23871 | 24090 |
| 22 | 24310 | 24531 | 24753 | 24976 | 25200 | 25425 | 25651 | 25878 | 26106 | 26335 |
| 23 | 26565 | 26796 | 27028 | 27261 | 27495 | 27730 | 27966 | 28203 | 28441 | 28680 |
| 24 | 28920 | 29161 | 29403 | 29646 | 29890 | 30135 | 30381 | 30628 | 30876 | 31125 |
| 25 | 31375 | 31626 | 31878 | 32131 | 32385 | 32640 | 32896 | 33153 | 33411 | 33670 |
| 26 | 33930 | 34191 | 34453 | 34716 | 34980 | 35245 | 35511 | 35778 | 36046 | 36315 |
| 27 | 36585 | 36856 | 37128 | 37401 | 37675 | 37950 | 38226 | 38503 | 38781 | 39060 |
| 28 | 39340 | 39621 | 39903 | 40186 | 40470 | 40755 | 41041 | 41328 | 41616 | 41905 |
| 29 | 42195 | 42486 | 42778 | 43071 | 43365 | 43660 | 43956 | 44253 | 44551 | 44850 |
| 30 | 45150 | 45451 | 45753 | 46056 | 46360 | 46665 | 46971 | 47278 | 47586 | 47895 |
| 31 | 48205 | 48516 | 48828 | 49141 | 49455 | 49770 | 50086 | 50403 | 50721 | 51040 |
| 32 | 51360 | 51681 | 52003 | 52326 | 52650 | 52975 | 53301 | 53628 | 53956 | 54285 |
| 33 | 54615 | 54946 | 55278 | 55611 | 55945 | 56280 | 56616 | 56953 | 57291 | 57630 |
| 34 | 57970 | 58311 | 58653 | 58996 | 59340 | 59685 | 60031 | 60378 | 60726 | 61075 |
| 35 | 61425 | 61776 | 62128 | 62481 | 62835 | 63190 | 63546 | 63903 | 64261 | 64620 |
| 36 | 64980 | 65341 | 65703 | 66066 | 66430 | 66795 | 67161 | 67528 | 67896 | 68265 |
| 37 | 68635 | 69006 | 69378 | 69751 | 70125 | 70500 | 70876 | 71253 | 71631 | 72010 |
| 38 | 72390 | 72771 | 73153 | 73536 | 73920 | 74305 | 74691 | 75078 | 75466 | 75855 |
| 39 | 76245 | 76636 | 77028 | 77421 | 77815 | 78210 | 78606 | 79003 | 79401 | 79800 |

| *n* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 40 | 80200 | 80601 | 81003 | 81406 | 81810 | 82215 | 82621 | 83028 | 83436 | 83845 |
| 41 | 84255 | 84666 | 85078 | 85491 | 85905 | 86320 | 86736 | 87153 | 87571 | 87990 |
| 42 | 88410 | 88831 | 89253 | 89676 | 90100 | 90525 | 90951 | 91378 | 91806 | 92235 |
| 43 | 92665 | 93096 | 93528 | 93961 | 94395 | 94830 | 95266 | 95703 | 96141 | 96580 |
| 44 | 97020 | 97461 | 97903 | 98346 | 98790 | 99235 | 99681 | 100128 | 100576 | 101025 |
| 45 | 101475 | 101926 | 102378 | 102831 | 103285 | 103740 | 104196 | 104653 | 105111 | 105570 |
| 46 | 106030 | 106491 | 106953 | 107416 | 107880 | 108345 | 108811 | 109278 | 109746 | 110215 |
| 47 | 110685 | 111156 | 111628 | 112101 | 112575 | 113050 | 113526 | 114003 | 114481 | 114960 |
| 48 | 115440 | 115921 | 116403 | 116886 | 117370 | 117855 | 118341 | 118828 | 119316 | 119805 |
| 49 | 120295 | 120786 | 121278 | 121771 | 122265 | 122760 | 123256 | 123753 | 124251 | 124750 |
| 50 | 125250 | 125751 | 126253 | 126756 | 127260 | 127765 | 128271 | 128778 | 129286 | 129795 |
| 51 | 130305 | 130816 | 131328 | 131841 | 132355 | 132870 | 133386 | 133903 | 134421 | 134940 |
| 52 | 135460 | 135981 | 136503 | 137026 | 137550 | 138075 | 138601 | 139128 | 139656 | 140185 |
| 53 | 140715 | 141246 | 141778 | 142311 | 142845 | 143380 | 143916 | 144453 | 144991 | 145530 |
| 54 | 146070 | 146611 | 147153 | 147696 | 148240 | 148785 | 149331 | 149878 | 150426 | 150975 |
| 55 | 151525 | 152076 | 152628 | 153181 | 153735 | 154290 | 154846 | 155403 | 155961 | 156520 |
| 56 | 157080 | 157641 | 158203 | 158766 | 159330 | 159895 | 160461 | 161028 | 161596 | 162165 |
| 57 | 162735 | 163306 | 163878 | 164451 | 165025 | 165600 | 166176 | 166753 | 167331 | 167910 |
| 58 | 168490 | 169071 | 169653 | 170236 | 170820 | 171405 | 171991 | 172578 | 173166 | 173755 |
| 59 | 174345 | 174936 | 175528 | 176121 | 176715 | 177310 | 177906 | 178503 | 179101 | 179700 |
| 60 | 180300 | 180901 | 181503 | 182106 | 182710 | 183315 | 183921 | 184528 | 185136 | 185745 |
| 61 | 186355 | 186966 | 187578 | 188191 | 188805 | 189420 | 190036 | 190653 | 191271 | 191890 |
| 62 | 192510 | 193131 | 193753 | 194376 | 195000 | 195625 | 196251 | 196878 | 197506 | 198135 |
| 63 | 198765 | 199396 | 200028 | 200661 | 201295 | 201930 | 202566 | 203203 | 203841 | 204480 |
| 64 | 205120 | 205761 | 206403 | 207046 | 207690 | 208335 | 208981 | 209628 | 210276 | 210925 |
| 65 | 211575 | 212226 | 212878 | 213531 | 214185 | 214840 | 215496 | 216153 | 216811 | 217470 |
| 66 | 218130 | 218791 | 219453 | 220116 | 220780 | 221445 | 222111 | 222778 | 223446 | 224115 |
| 67 | 224785 | 225456 | 226128 | 226801 | 227475 | 228150 | 228826 | 229503 | 230181 | 230860 |
| 68 | 231540 | 232221 | 232903 | 233586 | 234270 | 234955 | 235641 | 236328 | 237016 | 237705 |
| 69 | 238395 | 239086 | 239778 | 240471 | 241165 | 241860 | 242556 | 243253 | 243951 | 244650 |
| 70 | 245350 | 246051 | 246753 | 247456 | 248160 | 248865 | 249571 | 250278 | 250986 | 251695 |
| 71 | 252405 | 253116 | 253828 | 254541 | 255255 | 255970 | 256686 | 257403 | 258121 | 258840 |
| 72 | 259560 | 260281 | 261003 | 261726 | 262450 | 263175 | 263901 | 264628 | 265356 | 266085 |
| 73 | 266815 | 267546 | 268278 | 269011 | 269745 | 270480 | 271216 | 271953 | 272691 | 273430 |
| 74 | 274170 | 274911 | 275653 | 276396 | 277140 | 277885 | 278631 | 279378 | 280126 | 280875 |
| 75 | 281625 | 282376 | 283128 | 283881 | 284635 | 285390 | 286146 | 286903 | 287661 | 288420 |
| 76 | 289180 | 289941 | 290703 | 291466 | 292230 | 292995 | 293761 | 294528 | 295296 | 296065 |
| 77 | 296835 | 297606 | 298378 | 299151 | 299925 | 300700 | 301476 | 302253 | 303031 | 303810 |
| 78 | 304590 | 305371 | 306153 | 306936 | 307720 | 308505 | 309291 | 310078 | 310866 | 311655 |
| 79 | 312445 | 313236 | 314028 | 314821 | 315615 | 316410 | 317206 | 318003 | 318801 | 319600 |
| 80 | 320400 | 321201 | 322003 | 322806 | 323610 | 324415 | 325221 | 326028 | 326836 | 327645 |
| 81 | 328455 | 329266 | 330078 | 330891 | 331705 | 332520 | 333336 | 334153 | 334971 | 335790 |
| 82 | 336610 | 337431 | 338253 | 339076 | 339900 | 340725 | 341551 | 342378 | 343208 | 344035 |
| 83 | 344865 | 345696 | 346528 | 347361 | 348195 | 349030 | 349866 | 350703 | 351541 | 352380 |
| 84 | 353220 | 354061 | 354903 | 355746 | 356590 | 357435 | 358281 | 359128 | 359976 | 360825 |
| 85 | 361675 | 362526 | 363378 | 364231 | 365085 | 365940 | 366796 | 367653 | 368511 | 369370 |
| 86 | 370230 | 371091 | 371953 | 372816 | 373680 | 374545 | 375411 | 376278 | 377146 | 378015 |
| 87 | 378885 | 379756 | 380628 | 381501 | 382375 | 383250 | 384126 | 385003 | 385881 | 386760 |
| 88 | 387640 | 388521 | 389403 | 390286 | 391170 | 392055 | 392941 | 393828 | 394716 | 395605 |
| 89 | 396495 | 397386 | 398278 | 399171 | 400065 | 400960 | 401856 | 402753 | 403651 | 404550 |
| 90 | 405450 | 406351 | 407253 | 408156 | 409060 | 409965 | 410871 | 411778 | 412686 | 413595 |
| 91 | 414505 | 415416 | 416328 | 417241 | 418155 | 419070 | 419986 | 420903 | 421821 | 422740 |
| 92 | 423660 | 424581 | 425503 | 426426 | 427350 | 428275 | 429201 | 430128 | 431056 | 431985 |
| 93 | 432915 | 433846 | 434778 | 435711 | 436645 | 437580 | 438516 | 439453 | 440391 | 441330 |
| 94 | 442270 | 443211 | 444153 | 445096 | 446040 | 446985 | 447931 | 448878 | 449826 | 450775 |
| 95 | 451725 | 452676 | 453628 | 454581 | 455535 | 456490 | 457446 | 458403 | 459361 | 460320 |
| 96 | 461280 | 462241 | 463203 | 464166 | 465130 | 466095 | 467061 | 468028 | 468998 | 469965 |
| 97 | 470935 | 471906 | 472878 | 473851 | 474825 | 475800 | 476776 | 477753 | 478731 | 479710 |
| 98 | 480690 | 481671 | 482653 | 483636 | 484620 | 485605 | 486591 | 487578 | 488566 | 489555 |
| 99 | 490545 | 491536 | 492528 | 493521 | 494515 | 495510 | 496506 | 497503 | 498501 | 499500 |

### A Few Specimen Primes

In making up numbers for testing factorisation methods it is essential to employ factors known to be primes. In a book of this kind it is neither necessary nor practicable to tabulate long lists of primes in sequence and the following selection should provide enough variety for most purposes.

113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277

401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593

797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997

2309 2311 2333 2339 2341 2347 2351 2357 2371 2377 2381 2383 2389 2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477 2503 2521 2531 2539 2543

8803 8807 8819 8821 8831 8837 8839 8849 8861 8863 8867 8887 8893 8923 8929 8933 8941 8951 8963 8969 8971 8999 9001 9007 9011 9013 9029 9041 9043 9049

13709 13711 13721 13723 13729 13751 13757 13759 13763 13781 13789 13799 13807 13829 13831 13841 13859 13873 13877 13879 13883 13901 13903 13907 13913 13921 13931 13933 13951 13963

78901 78919 78929 78941 78977 78979 78989 79031 79037 79039 79043 79049 79063 79067 79103 79111 79133 79139 79147 79151 79153 79159 79181 79187 79193 79201 79229 79231 79241 79259

107309 107339 107347 107351 107357 107377 107441 107449 107453 107467 107473 107507 107509 107533 107563 107581 107599 107603 107609 107617 107621 107641 107647 107671 107687 107693 107699 107713 107717 107719

1000159 1000171 1000183 1000187 1000193 1000199 1000211 1000213 1000231 1000249 1000253 1000273 1000289 1000291 1000303 1000313 1000333 1000357 1000367 1000381 1000393 1000397 1000403 1000409 1000423 1000427 1000429 1000453 1000457 1000507

100004309 100004327 100004347 100004363 100004389 100004393 100004407 100004417 100004449 100004461 100004473 100004477 100004501 100004503 100004507 100004519 100004521 100004533 100004537 100004549 100004551 100004561 100004563 100004629 100004647 100004651 100004677 100004719 100004741 100004813

| $n$ | $2^n$ | $3^n$ |
|---|---|---|
| 2 | 4 | 9 |
| 3 | 8 | 27 |
| 4 | 16 | 81 |
| 5 | 32 | 243 |
| 6 | 64 | 729 |
| 7 | 128 | 2187 |
| 8 | 256 | 6561 |
| 9 | 512 | 19683 |
| 10 | 1024 | 59049 |
| 11 | 2048 | 177147 |
| 12 | 4096 | 531441 |
| 13 | 8192 | 1594323 |
| 14 | 16384 | 4782969 |
| 15 | 32768 | 14348907 |
| 16 | 65536 | 43046721 |
| 17 | 131072 | 129140163 |
| 18 | 262144 | 387420489 |
| 19 | 524288 | 1162261467 |
| 20 | 1048576 | 3486784401 |
| 21 | 2097152 | 10460353203 |
| 22 | 4194304 | 31381059609 |
| 23 | 8388608 | 94143178827 |
| 24 | 16777216 | 282429536481 |
| 25 | 33554432 | 847288609443 |
| 26 | 67108864 | 2541865828329 |
| 27 | 134217728 | 7625597484987 |
| 28 | 268435456 | 22876792454961 |
| 29 | 536870912 | 68630377364883 |
| 30 | 1073741824 | 205891132094649 |
| 31 | 2147483648 | 617673396283947 |
| 32 | 4294967296 | 1853020188851841 |
| 33 | 8589934592 | 5559060566555523 |
| 34 | 17179869184 | 16677181699666569 |
| 35 | 34359738368 | 50031545098999707 |
| 36 | 68719476736 | 150094635296999121 |
| 37 | 137438953472 | 450283905890997363 |
| 38 | 274877906944 | 1350851717672992089 |

| $n$ | $2^n$ | $3^n$ |
|---|---|---|
| 39 | 549755813888 | 4052555153018976267 |
| 40 | 1099511627776 | 12157665459056928801 |
| 41 | 2199023255552 | 36472996377170786403 |
| 42 | 4398046511104 | 109418989131512359209 |
| 43 | 8796093022208 | 328256967394537077627 |
| 44 | 17592186044416 | 984770902183611232881 |
| 45 | 35184372088832 | 2954312706550833698643 |
| 46 | 70368744177664 | 8862938119652501095929 |
| 47 | 140737488355328 | 26588814358957503287787 |
| 48 | 281474976710656 | 79766443076872509863361 |
| 49 | 562949953421312 | 239299329230617529590083 |
| 50 | 1125899906842624 | 717897987691852588770249 |

# ANSWERS TO THE EXERCISES

## Chap. 1

1. 10101101100111.

2. 2(11)67.

3. (10)(27)7.

4. (*a*) The digits 2, (11), 6, 7, expressed in the scale of 2—allowing for the (legitimate) addition of some 0's—are respectively 10, 1011, 0110, 0111.

   (*b*) The digits (10), (27), 7, similarly expressed are 1010, 11011, 0111. Compare Ans. 1.

5.

| | | | |
|---|---|---|---|
| 123 | 456 | 456 | ~~123~~ |
| 61 | 912 | 228 | ~~246~~ |
| 30 | ~~1824~~ | 114 | ~~492~~ |
| 15 | 3648 | 57 | 984 |
| 7 | 7296 | 28 | ~~1968~~ |
| 3 | 14592 | 14 | ~~3936~~ |
| 1 | 29184 | 7 | 7872 |
| | ——— | 3 | 15744 |
| | 56088 | 1 | 31488 |
| | | | ——— |
| | | | 56088 |

6. Since 707 = 7 × 101, apply the '$s + 1$' rule after separating $N$ into pairs of digits, thus: 45, 53, 31. Then $31 + 45 - 53 = 23$ = remainder.

**Chap. 2**

1. (*a*) × 13 and add. (*b*) × 30 and subtract.

```
21010101                           21010101
      13                                 30
--------                           --------
 2101023                            2100980
      39                                240
 -------                            -------
  210141                              20769
      13                                270
  ------                              -----
   21027                               1806
      91           10000000             180
   -----            9837131             ---
    2193           --------               0
      39             162869                       69801
    ----                  3                           7
     258            -------                     -------
    104              488607 = n               = 488607
    ---
    129 = 3 × 43.
```

2.

```
110999999   (997 = 1000 − 3)
        3
---------
 11299999
        3
 --------
  1329999
        3
  -------
   332999
        9
   ------
    33899
        9
    -----
     3989   Therefore the remainder is 1,
        9   and the quotient is
     ----
      998   111333 + 1 = 111334.
      997
      ---
        1
```

3. Since 167 × 6 = 1002, use a similar procedure to the above but in this case *add* the multiples of 2.

**Chap. 3**

1. 3/41 = ·07317 29/41 = ·70731
 7/41 = ·17073 30/41 = ·73170
 13/41 = ·31707

2. As with all recurrent cycles an algorithm—usually several—can always be found. I give the following because it differs markedly from those described in the text and shows something of the variety to be met with in this field.

If $n$ takes the successive values 1, 2, 3, . . . $n$, then $11(2^n - 2)$ defines the sequence 0, 22, 66, 154, 330, 682, 1386, etc. Dividing each term by $10^{2n}$ and summing, we have:

```
·00
   22
     66
      154
        330
          682
          1386
            2794
              5610
              11242
                22506
                  . . .   etc.
---------------------
·002267573696145124 . . .
```

$11(2^n - 2)$ is, of course equivalent to $22(2^{n-1} - 1)$; the latter part of this will become quite familiar.

**Chap. 4**

1. 3·1416.

2. By definition
$$\begin{aligned} F_1 &= F_3 - F_2 \\ F_2 &= F_4 - F_3 \\ F_3 &= F_5 - F_4 \\ &\ \ldots \\ F_{n-1} &= F_{n+1} - F_n \\ F_n &= F_{n+2} - F_{n+1} \end{aligned}$$

Adding all these equations together we have on the left hand side the sum of the first Fibonacci numbers, whilst the terms on the right sum to $F_{n+2} - F_2$.

Since $F_2 = 1$, the required sum is therefore $F_{n+2} - 1$.

**Chap. 6**

1. $1001001001 \times 111 = I_{12}$
   $100010001 \times 1111 = I_{12}$

   The factors common to both numbers are therefore those of $I_{12}$ omitting those of $I_3$ and $I_4$, (3, 11, 37, 101). Hence they are 7, 13, *and* 9901.

2. (See Tables 8 and 9)
   The sequence 91, 9091, 909091, 90909091, etc. occurs in the factorisations of $I_6$, $I_{10}$, $I_{14}$, . . . $I_{4k+1}$. Since 90909091 does not appear among the prime factors of $I_{18}$ it must therefore be composite.

3. $I_{12} = 3333 \times 33336667 = 3.7.11.13.37.101.9901$
   Since $3333 = 3.11.\ 101$,
   then $33336667 = 7.13.37.9901$.

**Chap. 7**

1. The eight numbers relatively prime to 20 are 1, 3, 7, 9, 11, 13, 17, and 19 and therefore by Euler's generalisation $n$ can take any of the values $20k + 1, 3, 7, 9,$ etc.
   Thus, for instance $7^8 - 1 = 5764800$
   and $19^8 - 1 = 16983563040$.

2. The index 12 appears at the following places in the table: $m = 13, 21, 26, 28, 36, 42$. Collectively these numbers contain the primes 2, 3, 7, and 13 and it follows that these are all factors of $5^{12} - 1$.
   (5 being relatively prime to 12).

3. $402 = 2.3.67$.
   $$\begin{aligned}\phi(402) &= 402(1 - 1/2)(1 - 1/3)(1 - 1/67)\\ &= 402 \times 1/2 \times 2/3 \times 66/67\\ &= 6 \times 1/3 \times 66 = 2 \times 66 = 132.\end{aligned}$$

**Chap. 9**

1. $$5x = 1001 - 9y$$
   Remainders on dividing by 5, 1    4
   Multiplying the integers 1 2 3 4
   by 4, removing multiples of 5; 4 3 2 1
   1 is in the fourth position, hence $y = 4$.
   Then $5x = 1001 - 36 = 965$.    $x = 193$.

2. For $z = 26 = m^2 + n^2$, the only positive integer values of $m$ and $n$ are 5 and 1.
   Then $x = m^2 - n^2 = 24$
   and $y = 2mn = 10$
   i.e. $24^2 + 10^2 = 26^2$.

**Chap. 10**

1. (*a*) 1. (*b*) 5. (Extrapolated from Tables 14*a*, *b*).

2. Divide each term as it appears, by 7; the remainder multiplied by three then provides the next term. In this way we get the sequence 1, 3, 2, 6, 4, 5, 1, 3, etc. The remainder thus appears as 1 when $n = 0, 6, 12, \ldots = 6k$ and therefore $3^{6k} - 1$ is always divisible by 7.

3. 5 and 8. (See Table 14*b*.)

**Chap. 11**

1. $99999999 = 10^8 - 1$
   $$\begin{aligned}&\text{Now} & 10^2 &\equiv -1 \pmod{101}\\ &\text{Therefore} & 10^8 &\equiv 1\\ &\text{or} & 10^8 - 1 &\equiv 0 \pmod{101}\end{aligned}$$

2. $$\begin{aligned}2^5 &= 32 \equiv 9 \pmod{23}\\ 2^{10} &\equiv 81 \equiv 12\\ 2^{11} &\equiv 24 \equiv 1\\ 2^{22} &\equiv 1. \text{ or } 2^{22} - 1 \equiv 0 \pmod{23}.\end{aligned}$$

3. Dividing throughout by 7 we find that 2908456 has the remainder 5, which is not a quadratic residue of 7. (*b*) is therefore not a square. Dividing *a*, *c*, *d*, *e*, by 11, (*e*) has the remainder 2, and hence is not a square.
   Ans. (*b*) and (*e*).

**Chap. 12**

1. 29.

```
16733)35699
      33466
       2233)16733
            15631
             1102)2233
                  2204
                    29)1102
                         87
                        232
                        232
                          0
```

2. It is easily seen that 3, 7, 11, 13, are not divisors so we set up

$$\Pi_{17\leqslant p\leqslant 29}(p) = 17.19.23.29 = 215441.$$

```
215441)1181027
       1077205
        103822)215441
               207644
                 7797)103822
                       7797
                       25852
                       23391
                        2461)7797
                             7383
                              414)2461
                                  2484
                                   
```

Therefore 23 is a factor. $-\ 23$

3.

```
         1 0 4 6²
     N = 1093709
         100
204       937
          816
2086     12109
         12516
           407
          2093 = (2 × 1046) + 1
          2500 = 50²
```

Therefore $N = 1047^2 - 50^2 = 1097 \times 997$.

**Chap. 13**

1. $15871 = 59 \times 269$.
$15853 = 83 \times 191$.
$15863 = 29 \times 547$.

2. $13333 = 67 \times 199$.
$548497 = 53 \times 79 \times 131$.

## by D. St. P. Barnard

### FIFTY 'OBSERVER' BRAIN-TWISTERS

'These are really excellent original puzzles.' *The Times Literary Supplement*

'This collection includes not only the detailed solutions but useful hints to put the reader on the right track if he is baffled at the first attempt. The problems are all ingenious and some are quite difficult, though they need only elementary mathematics and straightforward reasoning.' *Glasgow Herald*

13*s* 6*d net*

### ONE HUNDRED BRAINTWISTERS

*A second book of puzzles and problems*

Not only are the puzzles in this book a stimulating challenge to the reader's ingenuity, but the carefully explained solutions that accompany each problem contain many useful hints on how to set about reducing complex questions to simple techniques of common sense and reason.

'Mr. Barnard is no purveyor of old puzzles in new dress, but an original creator in this form.' *Mathematical Gazette* 21*s net*

*If you would like to receive*
*our announcement catalogues regularly*
*please write to*
*Faber & Faber Limited*
*London WC1*

## MAKERS OF MATHEMATICS

Alfred Hooper

'. . . Admirable . . . for it not only sets mathematics into the framework of an evolving society but also shows the development of mathematics to be a continual and thrilling adventure of ideas. . . . From a book of this kind certain types of student will learn more mathematics in a month than in a year of normal study, not because the drill is here but because the stimulus is.' *Further Education*

*Faber Paper Covered Editions* 15*s net*

## THE SCIENCE OF CHANCE

Horace C. Levinson

Life is a chancy business!

It is not merely in the toss of a coin or the turn of a card that Chance influences one's prospects. In nearly all spheres of life, success often depends on one's ability to 'assess the chances'.

Mere hunches and superstitions are not enough; Dr. Levinson treats Chance as a science. But there is no scientific jargon in the book. By starting off with simple questions of dice-throwing, poker hands, and roulette spins, the author paves the way to understanding how Chance affects the significance of statistics, the worth of opinion polls, the value of advertising campaigns, and the assessment of production methods.

In brief, Dr. Levinson teaches one how to take a chance—and when not to.

*Faber Paper Covered Editions* 12*s* 6*d net*

## 50 MATHEMATICAL PUZZLES AND ODDITIES

Nicholas E. Scripture

'This is a mathematical bran-tub in which oddments in arithmetic, algebra, geometry and a few less definable subjects can be fished out. They are ingenious, instructive, often amusing and where necessary illustrated.' *The Times Literary Supplement*

*Faber Paper Covered Editions* 6*s net*

## 50 WIT-SHARPENERS

Nicholas E. Scripture

For variety these puzzles are hard to beat—some will appeal to those who are fascinated by the properties of numbers, but there are also acrostics, word squares, alphametrics, codes and many others, all introduced with wit and clarity, so that the general reader as well as the confirmed puzzle addict is likely to find himself intrigued.

15*s net*

NUMBERS

L.F.Taylor